



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ PERIMETRU V EXTRÉMNÍCH PODMÍNKÁCH S VYUŽITÍM SENZOROVÝCH SÍTÍ

PROTECTING THE PERIMETER IN EXTREME CONDITIONS, USING SENSOT NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. JAKUB DAVID

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. ONDŘEJ KRAJSA, Ph.D.

BRNO 2013



**VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky
a komunikačních technologií**

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Jakub David

ID: 120770

Ročník: 2

Akademický rok: 2012/2013

NÁZEV TÉMATU:

Zabezpečení perimetru v extrémních podmínkách s využitím senzorových sítí

POKYNY PRO VYPRACOVÁNÍ:

Analyzujte možnosti využití různých typů senzorů a senzorových sítí pro detekci narušení perimetru. Navrhněte a realizujte bezdrátový senzorový uzel pro detekci narušení perimetru využitelný v bezdrátových senzorových sítích s nízkou spotřebou. Navrhněte komunikaci s řídicím prvkem a vyhodnocování jednotlivých událostí vyvolaných senzorem.

DOPORUČENÁ LITERATURA:

- [1] Catsoulis, John Designing embedded hardware. O'Reilly, 2005. xvi, 377 s. ISBN 0-596-00755-8
- [2] Váňa, Vladimír. Mikrokontroléry ATMEL AVR: programování v jazyce C.BEN - technická literatura, 2003. ISBN 80-7300-102-0
- [3] FRADEN, Jacob. Handbook of modern sensors: physics, designs, and applications. 4th ed. New York: Springer, 2010, xv, 663 s. ISBN 978-1-4419-6465-6.
- [4] EREN, Halit. Wireless sensors and instruments: networks, design, and applications. Boca Raton: CRC/Taylor & Francis, 2006, 297 s. ISBN 0-8493-3674-0.

Termín zadání: 11.2.2013

Termín odevzdání: 29.5.2013

Vedoucí práce: Ing. Ondřej Krajsa, Ph.D.

Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Výzkum popsáný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Abstrakt

Tato diplomová práce se zabývá teoretickým rozbořem a úvodem do problematiky bezdrátových senzorových sítí, popisem vybraných typů senzorů, výčtem jejich vlastností a principů činnosti pro detekci narušení perimetru. Dále je zde popsán návrh a realizace bezdrátového senzorového uzlu pro detekci narušení perimetru využitelný v bezdrátových senzorových sítích.

Abstract

This master thesis deals with the theoretical analysis of wireless sensor networks, a description of selected types of sensors, listing their features and principle of operation for intrusion detection perimeter. Then there is described design and implementation of a wireless sensor node for intrusion detection perimeter usable in wireless sensor networks.

Klíčová slova

WSN, ZigBee, 6LoWPAN, PIR, ultrazvukový senzor, SRF 08, optická závora, deRFnode, Dresden-Elektronik, AVR, ATmega 128RFA1

Key words

WSN, ZigBee, 6LoWPAN, PIR, ultrasonic module, SRF 08, optical barrier, deRFnode, Dresden-Elektronik, AVR, ATmega 128RFA1

Bibliografická citace

DAVID, J. *Zabezpečení perimetru v extrémních podmínkách s využitím senzorových sítí*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2013. 71 s. Vedoucí diplomové práce Ing. Ondřej Krajsa, Ph.D..

Prohlášení

Prohlašuji, že svou diplomovou práci na téma „Zabezpečení perimetru v extrémních podmínkách s využitím senzorových sítí“ jsem vypracoval samostatně pod vedením vedoucího semestrální práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené semestrální práce dále prohlašuji, že v souvislosti s vytvořením této semestrální práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následku porušení ustanovení § 11 a následujících autorského zákona c. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne 11. 12. 2012

podpis autora:

Poděkování

Děkuji vedoucímu diplomové práce Ing. Ondřejovi Krajsovi, Ph.D. za velmi užitečnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé diplomové práce. Dále bych chtěl poděkovat výzkumnému centru SIX v jehož laboratořích byla práce realizovaná. A v neposlední řadě mé rodině a přítelkyni za podporu a trpělivost při psaní této práce.

V Brně dne

.....

(podpis autora)

OBSAH

Obsah

Seznam obrázků

Seznam tabulek

1 KAPITOLA	
ÚVOD	1
2 KAPITOLA	
ZABEZPEČENÍ PERIMETRU, POPIS STÁVAJÍCÍHO ZABEZPEČENÍ	2
2.1 Počátky elektronických zabezpečovacích zařízení	2
2.2 Moderní řešení	2
2.3 Zabezpečení muničního skladu AČR	3
2.4 Použité technologie	5
3 KAPITOLA	
SEZNÁMENÍ S BEZDRÁTOVÝMI SENZOROVÝMI SÍTĚMI	6
3.1 Znaky WSN	7
3.2 Architektura WSN.....	7
3.3 Standard IEEE 802.15.4	9
3.3.1 Linková vrstva.....	9
3.3.1.1 Definice typu zařízení.....	9
3.3.1.2 Adresace	10
3.3.1.3 Topologie	10
3.3.1.4 Řízení přístupu	11
3.3.2 Fyzická vrstva	11
3.4 Protokol ZigBee	12
3.5 Protokol 6LoWPAN	13
3.5.1 Vrstvový model.....	14

3.6	Energetická náročnost WSN sítí	15
3.6.1	Principy redukce energetické spotřeby	15
3.6.1.1	Na fyzické vrstvě	16
3.6.1.2	Na linkové vrstvě	17
4	KAPITOLA	
	POPIS PROBLÉMU A SPECIFIKACE CÍLE	21
5	KAPITOLA	
	NÁVRH ŘEŠENÍ	22
5.1	Analýza detektorů	23
5.1.1	Rozdělení detektorů z fyzikálního principu	23
5.1.2	Optická závora	24
5.1.2.1	Konstrukce	24
5.1.2.2	Použití	25
5.1.2.3	Falešné poplachy	25
5.1.3	Pasivní infračervené detektory	26
5.1.3.1	Konstrukce	27
5.1.3.2	Použití	27
5.1.3.3	Falešné poplachy	28
5.1.4	Ultrazvuková čidla	28
5.1.4.1	Konstrukce	28
5.2	Komunikační rozhraní detektorů	29
5.2.1	Sběrnice I2C	29
5.2.2	Rozhraní SPI	30
5.3	Výběr detektorů	31
5.3.1	PIR smd modul 172500	31
5.3.2	Ultrazvukový senzor SRF 08	32
5.3.3	Optická závora	33
5.3.4	Akcelerometr BMA150	33
5.4	Návrh koncového zařízení	34
5.4.1	Popis a schéma koncového zařízení	35
5.4.2	Energetická spotřeba koncového zařízení	37
5.4.2.1	Alternativní zdroj energie	37

6	KAPITOLA KONSTRUKCE	40
6.1	Popis návrhu zapojení	40
6.2	Návrh plošného spoje	41
6.2.1	Technické požadavky na DPS:	42
7	KAPITOLA FIRMWARE	43
7.1	Bezdrátový senzorový uzel.....	43
7.2	Koordinátor sítě.....	45
8	KAPITOLA ZÁVĚR	46
	Literatura	47
	Seznam zkratek	51
	Seznam příloh	53

SEZNAM OBRÁZKŮ

Obr. 1.:Zabezpečení perimetru muničního skladu. [1].....	3
Obr. 2.: Zabezpečení skladu pomocí infračervených závor. [1]	4
Obr. 3.: Použití WSN. [2] [3] [4]	6
Obr. 4: Architektura WSN sítě [7]	8
Obr. 5: Topologie typu HVĚZDA[6]	10
Obr. 6: Topologie typu MESH[6]	11
Obr. 7: Topologie typu STROM	13
Obr. 8:Vrstvový model 6LoWPAN [5]	14
Obr. 8: Napájení rádiové části.	16
Obr. 10: Asynchronní pracovní režim. [26].....	18
Obr. 11: Synchronní pracovní režim. [26].....	19
Obr. 12: Návrh zabezpečení, topologie hvězda	23
Obr. 13: Uskupení IR závor.[8]	25
Obr. 14: Princip PIR detektoru [11].....	26
Obr. 12: Pyroelement [15]	27
Obr. 16: Princip ultrazvukového senzoru [14].....	28
Obr. 17: Princip I2C sběrnice[5]	29
Obr. 18: Ukázka odesílání dat[27]	30
Obr. 19: Princip sběrnice SPI. [28]	31
Obr. 20: PIR smd modul 172500 [15].....	31
Obr. 21:SRF08 [19].....	33
Obr. 22: deRFgateway-1TNP2 [21]	35

Obr. 23: Rozmístění dvou senzorových uzlů.....	35
Obr. 24: Blokové schéma zapojení koncového uzlu se senzory	36
Obr. 24: Fotovoltaický článek [30]	38
Obr. 25: Windbelt [31]	39
Obr. 26: Bezdrátový senzorový uzel	41
Obr. 27: Vývojový diagram senzorového uzlu	44
Obr. 28: Vývojový diagram koordinátora sítě	45

SEZNAM TABULEK

Tab. 1: Definované frekvenční kanály[6]	12
Tab. 2: Terminologie ZigBee a IEEE 802.15.4 [5].....	13
Tab. 3: Typy baterií a jejich parametry [25]	17
Tab. 4: Srovnání MAC protokolů (asynchronních) [26]	19
Tab. 5: Srovnání MAC protokolů (asynchronních) [26]	20
Tab. 6: Parametry PIR senzoru [15].....	32
Tab. 7: Parametry ultrazvukového senzoru [16]	32
Tab. 8: Parametry optické závory [18][29].....	33
Tab. 9: Parametry BMA150 [20]	34

1 KAPITOLA

ÚVOD

Již od nepaměti se lidé zabývají snahou o zabezpečení svého majetku, věcí a objektů. Jednotlivá zařízení sloužící k zabezpečení prošla dlouhou etapou inovací a vylepšení závislých na důvtipu samotných tvůrců těchto zabezpečovacích zařízení až k moderním zařízením, pracujících s vysokou spolehlivostí.

Rozhodující vliv v oblasti zabezpečení měl příchod polovodičů a s tím i použití integrovaných obvodů. Výsledkem bylo především zjednodušení elektronické části zařízení. Zvětšení spolehlivosti a miniaturizace celkového provedení. V této době se začínaly vyvíjet také senzory, bez kterých by zabezpečovací technika nemohla existovat. Senzor převádí snímanou veličinu nebo měřený jev a pomocí vyhodnocovací elektroniky informaci zpracuje a vyhodnotí. Systém, který sám dokáže na základě předem dané logiky učinit závěr, zda se jedná například o narušení prostoru nebo o planý poplach, lze zařadit do kategorie inteligentního senzoru. Právě tato samostatnost senzorů má největší vliv na správnou funkčnost zabezpečovacího zařízení.

Cílem této práce je tedy navrhnout senzorový uzel, který bude schopen zabezpečit perimetr a tím také střežit daný prostor. Práce začíná krátkým úvodem do problematiky zabezpečení prostoru a bezdrátových sítí. Dále následují kapitoly popisující návrh a konstrukci řešení. Pro opravdu vysokou spolehlivost zabezpečovacího systému je zvoleno několik typů senzorů pracujících na odlišných principech. Navržený senzorový uzel je bezdrátové zařízení a tudíž je zde kladen důraz na nízkou spotřebu použitých senzorů.

2 KAPITOLA

ZABEZPEČENÍ PERIMETRU, POPIS STÁVAJÍCÍHO ZABEZPEČENÍ

Tato kapitola pojednává o zhodnocení a posouzení stávajících řešení daného problému, jak byl řešen jinými autory. Zhodnocení, výhody a nevýhody daného návrhu a různé typy možností zabezpečovacích systémů.

2.1 Počátky elektronických zabezpečovacích zařízení

Bezpochyby počátkem elektronických zabezpečovacích zařízení byl zcela jistě obyčejný elektrický obvod, složený ze spínače, napájení a poplašného zařízení, například žárovka nebo zvonek. Principiálně jednoduché řešení, spínač umístěný u vstupu do objektu například na dveřích se sepnul, pokud byly dveře otevřeny, a vyvolal alarm. Princip tohoto zabezpečení není příliš vhodný a potýká se s mnoha nedostatky. Jedním z nich je možnost vyřazení z provozu jednoduchým přerušením obvodu, tedy stačí, aby narušitel přestříhl vodič a zařízení není schopno žádným způsobem narušitele detekovat.

2.2 Moderní řešení

Dnes se již používají mnohem složitější a komplikovanější zařízení než jednoduchý obvod, ale princip zůstal stejný. Stále se jedná o senzor (spínač) a akční prvek (žárovka), ale v modernější podobě. Zařízení ovládaná mikrokontrolerem dokážou realizovat řadu funkcí, jako je předcházení planým poplachům, pokusy o zneškodnění zařízení a podobně. Hlavním požadavkem je vysoká spolehlivost zabezpečovacího zařízení, jednak proti již zmíněným sabotážím a dále proti extrémním podmínkám a rozmarům přírody. Pro splnění těchto požadavků jsou zabezpečovací zařízení doplněna o různé typy senzorů, pracujících na odlišných principech a tím znásobení

spolehlivosti. Tato zařízení již jsou schopna komunikovat s počítačem, což usnadňuje jak práci obsluhy zabezpečovacích zařízení, tak i výrobci. Výrobce se tak nemusí namáhat s konstrukcí kompletního zařízení a tím i zvýšení ceny produktu, ale stačí pouze vytvořit komunikační rozhraní a uživatelské prostředí. Počítač komunikuje se zabezpečovacím zařízením samostatně dle pokynů obsluhy. Výhoda je také v možnosti archivace dat na záložních discích, která jsou centrální jednotkou vyslána do PC. Spojení zařízení s PC je možno dosáhnout autonomního zařízení, které pracuje samostatně i bez stálého dozoru obsluhy.

2.3 Zabezpečení muničního skladu AČR

Jedním z objektů, které potřebují nejmodernější a nejlépe provedené zabezpečení prostoru jsou zcela jistě muniční sklady armády České republiky, ve kterých je uskladněna munice od dělostřeleckých nábojů přes náboje do ručních zbraní až po granáty.



Obr. 1.: Zabezpečení perimetru muničního skladu. [1]

Střežení takovýchto objektů není snadné a nelze se u nich spoléhat pouze na inteligenci celého zabezpečovacího zařízení, ale je nutné do procesu zapojit i tzv. lidský faktor. Osoba, která situaci monitoruje, ještě zvlášť posoudí, jestli se jedná o vniknutí do areálu nebo ne. Jeden z takovýchto komplexů AČR je skryt v lesích u Hostašovic na Novojičínsku. [1]

Objekt je střežen po celém svém obvodu kombinací několika typů senzorů a kamerových systémů umístěných na sloupech (Obr. 1). Tyto sloupy mají mezi sebou velmi malé rozestupy, přibližně 5 m a to právě z důvodu eliminace pokusu narušitele vyřadit z provozu jeden nebo i více z nich. I přestože v dnešní době existuje spousta moderních senzorů a detektorů přítomnosti je v takovýchto podmínkách nutnost použití videokamer nejen pro denní, ale i noční vidění. Pokud senzory zaznamenají narušitele, obraz z videokamer se okamžitě přepne na příslušný sektor a osoba sedící v řídící místnosti okamžitě na monitorech situaci sleduje. Tím se eliminují téměř veškeré plané poplachy, které mohou nastat. Takovéto zabezpečení objektů nepatří mezi špičku jen u nás, v České republice, ale také ve světě a je schopna jej provést pouze jedna tuzemská společnost. [1]



Obr. 2.: Zabezpečení skladu pomocí infračervených závor. [1]

2.4 Použité technologie

Jelikož se jedná o vojenský prostor, tak není nijak možné zjistit jak přesně a jakými typy senzorů je objekt jištěn. Díky tomu, že se jedná o pevné objekty, tak zde není podmínka mobility zabezpečovacího zařízení, což velice zjednodušuje možnosti napájení a přijímání signálů ze senzorů. A také rozšiřuje množství použitelných typů senzorů pro perimetrickou ochranu, jako jsou například:

- Infračervené závory
- Mikrovlnné bariéry
- Zemní tlakové hadice
- Rotující lasery
- Optická vlákna
- Kamerový systém
 - Výhody: umožňuje vzdálený dohled, dozírající osoba má o objektu celkový přehled a může upozorovat hrozbu mnohem dříve, minimum planých poplachů
 - Nevýhody: vysoká pořizovací cena, velká energetická náročnost, vysoké požadavky na šířku pásma sítě, potřeba osoby obsluhující kamerový systém

3 KAPITOLA

SEZNÁMENÍ S BEZDRÁTOVÝMI SENZOROVÝMI SÍTĚMI

Bezdrátová senzorová síť (WSN) je systém složený ze senzorických a řídicích prvků, které mezi sebou komunikují pomocí rádiového rozhraní, většinou za účelem monitorování prostředí. Dnes už WSN můžeme doslova potkat na každém kroku.

- Monitorování prostředí – požáry, stav sněhu na obtížně přístupných místech, záplavy, pohyb zvěře.
- Průmyslová diagnostika – měření stavu opotřebování jednotlivých dílů strojů, systém přenášející data o pohybu vozidel MHD
- Hlídaní infrastruktury – distribuční energetické sítě, rozvody pitné vody.
- Vojenské účely – monitorování vojáků území, střežení objektů
- Inteligentní budovy – ovládání osvětlení, vytápění, zabezpečení a multimediální zařízení



Obr. 3.: Použití WSN. [2] [3] [4]

Typický WSN prvek je v režimu spánku téměř 99% celkového času. Úkolem senzorových sítí je měření okolních fyzikálních parametrů a poté tato data odesílat na výchozí bránu sítě, případně na povel uživatele ovládat dostupné periferie. [5]

3.1 Znaky WSN

Díky obrovské miniaturizaci elektronických zařízení a se zvyšujícím se výpočetním výkonem a paměťovým úložištěm dnešních mikrokontrolérů se do popředí senzorických technologií dostávají zařízení definovaná dle standardu IEEE 802.15.4. Tato zařízení disponují velikostí nepřesahující rozměry dnešních mobilních telefonů, přičemž dosahují dostatečných komunikačních a výpočetních výkonů pro požadované řídicí a senzorické aplikace. Jejich charakteristické znaky jsou [5]:

- nízká přenosová rychlost v řádech kb/s (pro senzorické úlohy naprosto dostačující) a malé datové pakety
- velký počet prvků v síti (redundance) oproti WLAN (wireless local area network)
- nízká cena
- velmi nízký proudový odběr a dlouhá výdrž zařízení, prvky v síti jsou napájeny z baterie nebo alternativních zdrojů energie
- malé rozměry
- spolehlivý a šifrovaný přenos dat
- schopnost samoopravy topologie sítě pokud dojde k výpadku určitého prvku
- provoz v bezlicenčním pásmu
- nenáročná instalace

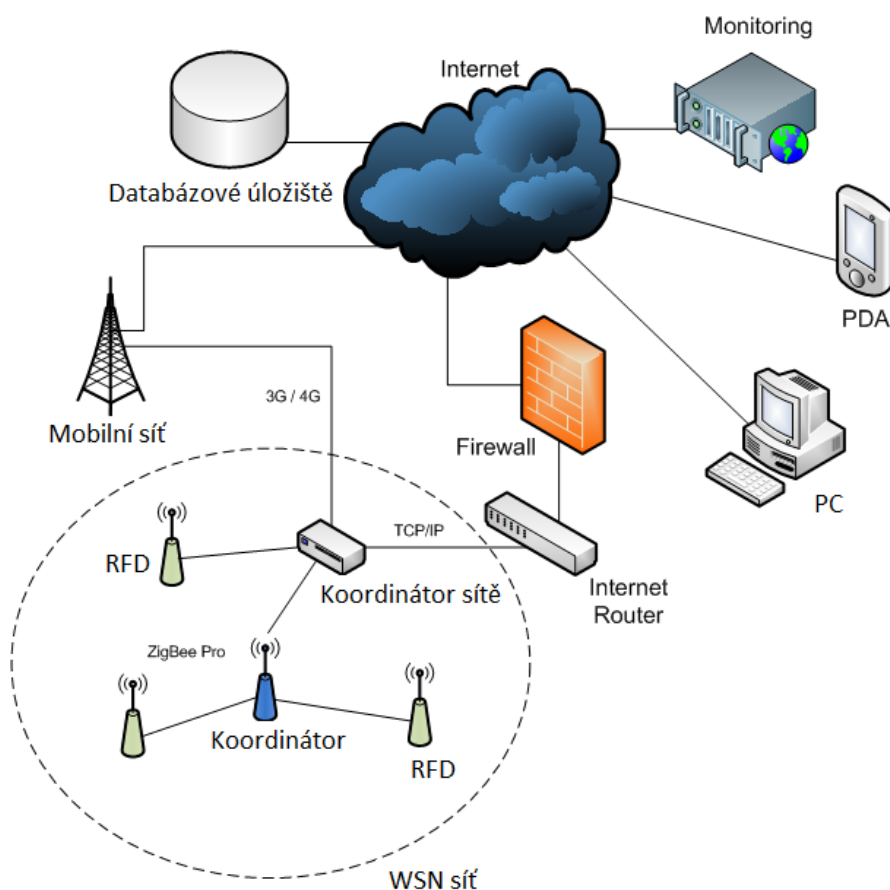
3.2 Architektura WSN

WSN síť je složena z několika částí. Základem jsou senzorové uzly (nodes) neboli také koncová zařízení, jejichž funkcí je zaznamenávání dat pomocí svých senzorů. Senzorový uzel je schopen data poslat svému sousedovi, se kterým má spojení a takto je přeposílat dál sítí směrem k výchozí bráně sítě. Na nejnižší úrovni jsou mezi sebou

navzájem propojené jednotlivé senzory, které mohou být rozděleny do skupin. Tato skupina se nazývá senzorové pole. [5]

Senzorová pole jsou připojena prostřednictvím jednoho nebo více uzlů k bráně, která představuje rozhraní mezi senzorovým polem a tranzitní sítí. Součástí základnové stanice může být databázové úložiště, kde dochází k ukládání dat získaných ze senzorů. Připojení základnové stanice k síti internet, bývá pomocí WAN sítě (Obr 4).

Díky tomuto se tedy správa senzorové sítě nemusí nalézat přímo v místě použití senzorové sítě, ale může probíhat odkudkoliv. Další možností jak spravovat senzorovou síť je pomocí přenosných zařízení, zde může komunikace probíhat přímo v místě senzorové sítě a obsluha má k dispozici jak nejnovější údaje získané ze senzorů, tak i přehled o jejím stavu. Obsluha si sama v přenosném zařízení vybírá, které ze změřených parametrů chce monitorovat. [5]



Obr. 4: Architektura WSN sítě [7]

3.3 Standard IEEE 802.15.4

Standard 802.15.4 pochází od neziskové organizace IEEE (Institute of Electrical and Electronics Engineers) pracovní skupiny číslo 4. Tato organizace vyvinula již řadu úspěšných produktů bezdrátových technologií, jako jsou wi-fi, bluetooth a wimax. Organizace všechny své produkty poskytuje bezlicenčně k dispozici, což zásadně napomáhá k rychlému použití v praxi. [5]

Standard 802.15.4 je základem téměř všech bezdrátových senzorových sítí o nízkém výkonu a malé přenosové rychlosti. Norma definuje maximální přenosovou rychlost 250 kb/s a maximální vysílací výkon 1 mW. Prvky pracující na této normě jsou schopné komunikovat běžně na několik desítek až stovek metrů, je možné ale dosáhnout i několika kilometrů. [6]

Norma IEEE 802.15.4 specifikuje pouze dvě vrstvy:

- Linkovou vrstvu – MAC
- Fyzickou vrstvu – PHY

3.3.1 Linková vrstva

Linková vrstva má na starost tyto následující úkoly:

- Typ zařízení (RFD/FFD)
- Adresování zařízení
- Synchronizace zařízení podle Beacon rámce
- Typ topologie (peer-to-peer/hvězda)
- Vyhrazování času pro komunikaci
- Přihlášení a odpojování zařízení k síti
- Řízení přístupu k bezdrátové síti

3.3.1.1 Definice typu zařízení

Norma definuje pouze dva typy:

FFD (Fully Function Device) – plně funkční zařízení schopné vykonávat všechny režimy v síti a může komunikovat se všemi prvky v síti. Může sloužit jako koordinátor

sítě, koordinátor nebo koncové zařízení. Koordinátor sítě řídí celou síť a zároveň pracuje jako i brána do jiných sítí a v každé síti se může nacházet pouze jen jeden. Koordinátor je zařízení, které je schopné směřovat data od koncového prvku směrem k jinému prvku v síti. [5]

RFD (Reduced Function Device) – zařízení s redukovanými funkcemi je senzorický a komunikační uzel, který může pouze data sbírat a posílat je koordinátorovi. RFD je pouze koncový uzel a nemůže komunikovat přímo s jiným koncovým RFD uzlem, tato komunikace mezi dvěma RFD koncovými zařízeními může probíhat pouze přes koordinátora. [5]

3.3.1.2 Adresace

Ve WSN sítích definovaných normou 802.15.4 je každému zařízení přidělena, buďto manuálně nebo koordinátorem sítě, unikátní adresa. Tyto adresy mohou být základní (16-bit adresování) nebo rozšířené (64-bit adresování). Pokud je zvoleno rozšířené adresování množství prvků v síti může stoupnout až na $1,8 \cdot 10^{19}$. [6]

3.3.1.3 Topologie

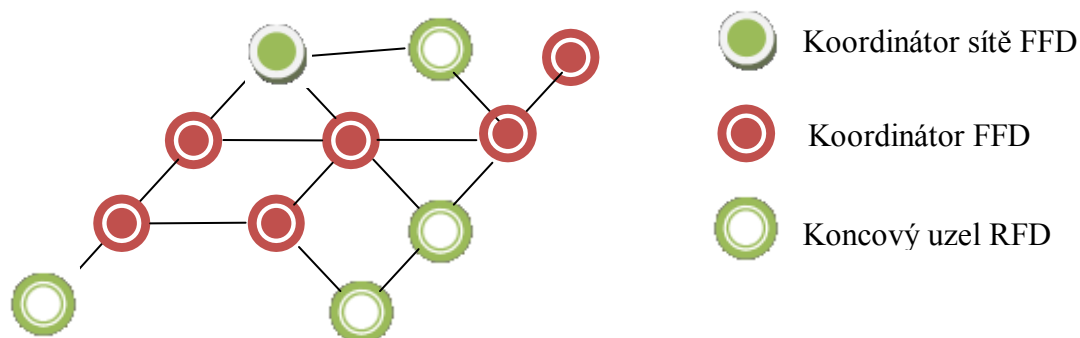
Topologie definované tímto standardem jsou pouze dvě, peer-to-peer a hvězda (star). U topologie hvězda (Obr. 5) komunikuje každé zařízení pouze s koordinátorem sítě. V síti je jeden koordinátor sítě a několik koncových zařízení. Koncová zařízení mohou být jak plně funkční zařízení, tak zařízení s redukovanými funkcemi. [6]



Obr. 5: Topologie typu HVĚZDA[6]

Druhá definovaná topologie je typu peer-to-peer (mesh), v této topologii zařízení FFD komunikují přímo mezi sebou a nemusí k tomu využívat koordinátora sítě. Uzly FFD tak pracují v podstatě jako směrovače pro komunikaci dvou koncových uzlů

a zařízení RFD slouží pouze jako koncový uzel a nemá schopnost směrovat, proto ke komunikaci využívají uzlů typu FFD. Standard IEEE 802.15.4 nedefinuje žádný směrovací protokol, k tomuto se využívá například protokol ZigBee. [6]



Obr. 6: Topologie typu MESH[6]

3.3.1.4 Řízení přístupu

Řízení přístupu k bezdrátovému kanálu po standardu IEEE 802.15.4 je pomocí metody detekce nosné s podporou vyhýbání kolizí – CSMA-CA (Carrier Sense Multiple Access with Collision Detection). Tuto metodu, až na pár výjimek, využívají jak zařízení typu FFD tak i typu RFD. [5]

3.3.2 Fyzická vrstva

Fyzická vrstva je rozhraní mezi linkovou vrstvou a přenosovým médiem, v tomto případě rádiovým spojením. V rádiovém pásmu IEEE 802.15.4 využívá tři bezlicenční pásma, která jsou omezená (typem modulace, vysílacím výkonem, střídou vysílání, adt.).

Fyzická vrstva se stará o tyto procesy:

- Příjem a přenos dat
- Zapnutí a vypnutí vysílače
- Výběr frekvenčního kanálu
- Zjištění volného kanálu

- Určení kvality přijímaných dat pomocí LQI (Link Quality Indication)

Norma definuje frekvenční kanály podle čísla kanálu a stránky kanálu. Stránka kanálu určuje typ použité modulace na daných frekvenčních kanálech (viz Tab. 1), zde jsou uvedeny pouze první tři stránky. Celkem je ve třech pásmech (868 MHz, 915 MHz a 2,4 GHz) vyhrazeno 27 frekvenčních kanálů. [6]

Tab. 1: Definované frekvenční kanály[6]

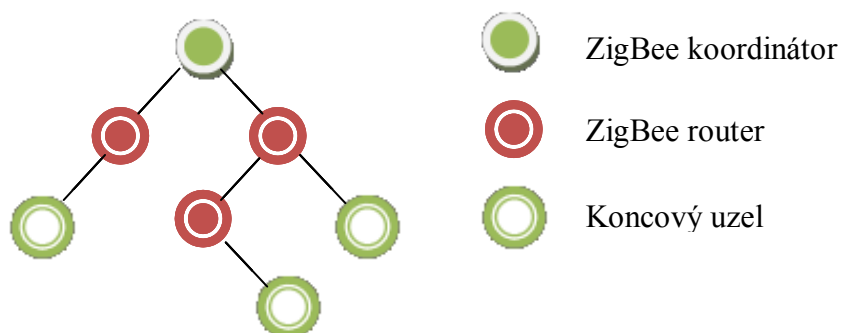
Stránka	Číslo kanálů	Frekvence	Modulace	Přenosová rychlost
0	0	868 MHz	BPSK	20 kb/s
	1-10	915 MHz	BPSK	40 kb/s
	11-26	2,4 GHz	O-QPSK	250 kb/s
1	0	868 MHz	ASK	251 kb/s
	1-10	915 MHz	ASK	252 kb/s
	11-26	rezervováno	-	-
2	0	868 MHz	O-QPSK	100 kb/s
	1-10	915 MHz	O-QPSK	250 kb/s
	11-26	rezervováno	-	-

3.4 Protokol ZigBee

Protokol ZigBee používá standard IEEE 802.15.4 a rozšiřuje jej o další vrstvy, síťovou (NWK layer) a aplikační vrstvu (APS layer) a o služby pro zabezpečení komunikace. ZigBee protokol je schopen provádět místo jedno skokové komunikace více skokovou komunikaci, tzn., že dvě zařízení mohou spolu komunikovat i když nejsou v přímém rádiovém dosahu. Další jeho vlastností je schopnost zabezpečit komunikaci pomocí šifrování. Tento protokol našel uplatnění především u inteligentních budov a v automatizaci domácnosti.

ZigBee na rozdíl od IEEE 802.15.4 definuje navíc i topologii typu strom (tree), ostatní topologie zůstávají stejné. Liší se pouze jejich terminologie, která se nachází níže, v tabulce 2. Základní charakteristikou stromové struktury je, že pro každý prvek v síti existuje pouze jedna spojitá cesta k libovolnému dalšímu prvku, a to přes prvky nacházející se mezi nimi. Uzly ležící mezi výchozím a cílovým prvkem slouží

k přeměrování zprávy směrem ke koordinátoru. Z toho vyplývá i nevýhoda stromové topologie. Pokud přestane pracovat jeden uzel, tak celá větev stromu nacházející se pod tímto uzlem nebude moci komunikovat s koordinátorem, což je patrné z Obr.7. [5]



Obr. 7: Topologie typu STROM

Tab. 2: Terminologie ZigBee a IEEE 802.15.4 [5]

ZigBee	ZigBee koordinátor (ZC)	ZigBee router (ZR)	Koncový uzel (ZED)
IEEE 802.15.4	Síťový koordinátor	Koordinátor	Koncový uzel

Znaky ZigBee:

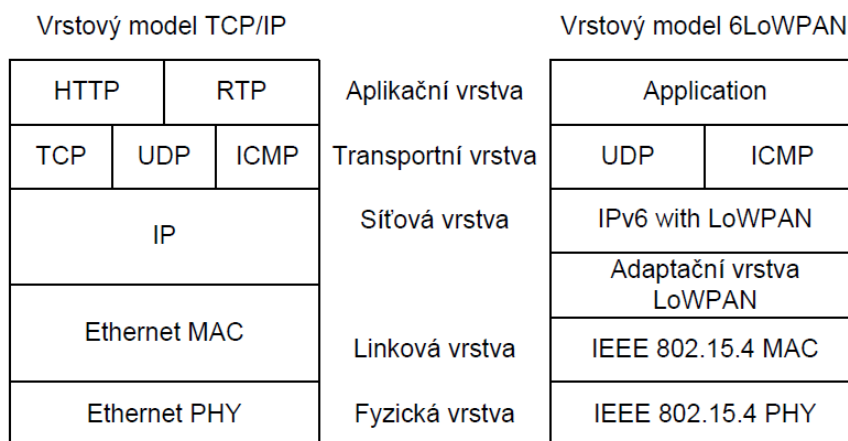
- Rozšířitelná a flexibilní síť
- Spolehlivost komunikace při nízké spotřebě
- Jednotné rozhraní pro koncové aplikace
- Jedno skoková a více skoková topologie
- Více sítí v jednom společném prostoru

3.5 Protokol 6LoWPAN

6LoWPAN (IPv6 Low power Wireless Personal Area Networks) je protokol pracující s protokolem IPv6 ve WSN sítích a dovoluje připojit tedy obrovské množství zařízení, a to díky zavedení adaptační vrstvy je možno komunikovat přes IPv6. Adaptační vrstva umožňuje fragmentaci, kompresi hlaviček rámců a tedy snížení energetické náročnosti přenosu dat. [5]

3.5.1 Vrstvový model

Vrstvový model u protokolu 6LoWPAN vychází z modelu TCP/IP a až na pár změn je téměř shodný (viz Obr. 8). [5]



Obr. 8: Vrstvový model 6LoWPAN [5]

Aplikační vrstva umožňuje přístup jednotlivým aplikacím k systému a zajišťuje jejich spolupráci.

Transportní vrstva se stará o samotný přenos dat. Zejména využívá protokolu UDP (User Datagram Protocol) pro přenos dat a protokolu ICMP (Internet Control Message Protocol) pro odesílání chybových zpráv (ping, atd).

Síťová vrstva obstarává správu sítě přes protokol SNMP (Simple Network Management Protocol), sestavuje spojení a obsahuje protokoly pro směrování v síti.

Adaptační vrstva definuje způsob komunikace v IPv6 síti a zajišťuje kompresi hlaviček, fragmentaci částí, přesměrování na síťovou vrstvu a IPv6 pakety uzpůsobuje na rámce pro WSN síť.

Linková vrstva zajišťuje přístup k médiu, MAC adresaci, opravu chyb, vytváření rámců, řízení toku rámců. Určuje přístupovou metodu CSMA/CA a zda uzel bude data přenášet v asynchronním či synchronním režimu.

Fyzická vrstva je definovaná podle standardu IEEE 802.15.4 a skládá se z vysílače (transmitter) a přijímače (receiver) pro bezdrátový přenos.

3.6 Energetická náročnost WSN sítí

V bezdrátových senzorových sítích je spotřeba energie velice důležitým aspektem. Koncové senzorové uzly jsou většinou používány v místech se zhoršeným přístupem k napájecí síti, a proto se využívají k jejich napájení akumulátory. Většinu energie v senzorových prvcích spotřebovává hardware, je proto nezbytné v nízkoenergetických systémech, pro dosažení největší úspory energie, s tímto počítat již při návrhu senzorového uzlu. Spotřeba elektrické energie každého jednotlivého WSN prvku je složena z dílčích součtů spotřeb energie při vykonávání jednotlivých úkonů. Můžeme je rozdělit na tyto tři [23]:

- **Sbírání a měření hodnot** - při sběru dat záleží na použitém typu senzoru, na veličině, která má být měřena a na principu jejího snímání. Různé typy senzorů založené na různých principech mají různou spotřebu energie.
- **Výpočetní operace** - spotřeba při výpočetních operacích se odvíjí od spotřeby výpočetního bloku, tedy od mikrokontroléru. Tento výpočetní blok je v chodu při každé činnosti, kterou se uzel zabývá. Zvláště pak při sběru a měření dat a jejich následném zpracování.
- **Komunikace** - spotřeba senzorového uzlu při komunikaci s dalším prvkem sítě je složena ze spotřeby při přijímání dat a při vysílání dat.

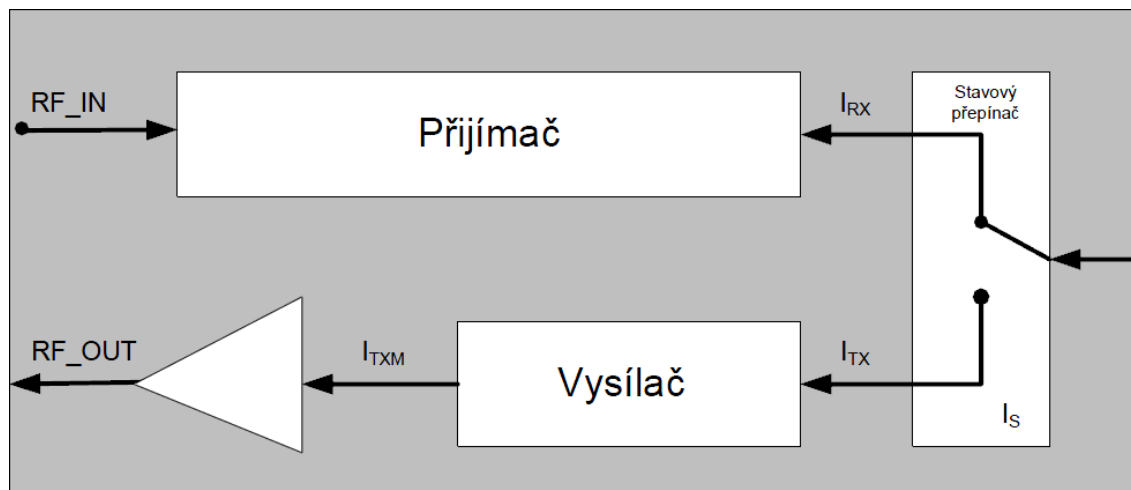
Spotřeba elektrické energie se řeší jak na fyzické tak i na linkové vrstvě. Spotřeba ve WSN sítích je závislá na spotřebě při dílčích činnostech senzorového uzlu. Největší spotřebu uzel zaznamenává při přijímání a odesílání nasbíraných dat, tedy při komunikaci. Naopak energetická náročnost výpočetního bloku pracujícího při každém úkonu je výrazně nižší [23].

3.6.1 Principy redukce energetické spotřeby

Základem pro realizaci systému s nízkou energetickou náročností je vybrání vhodné topologie WSN a komunikačních protokolů. Již bylo vytvořeno velké množství systémů zabývajících se touto problematikou (např. ZigBee, 6LoWPAN atd.), které se liší právě v typu topologie a ve volbě různých komunikačních protokolů. Dále bude popis snížení energetické náročnosti věnován pouze protokolu 6LoWPAN [24].

3.6.1.1 Na fyzické vrstvě

Na fyzické vrstvě je řešeno snížení spotřeby energie zvolením optimálního způsobu čerpání energie při napájení prvků WSN sítě. Pro napájení bezdrátových sensorových uzlů se používají především akumulátory, které mohou být doplněny o dobíjecí obvody. Podstatným významem v šetření energie je schéma napájení skládající se z režimu přenosu zpráv, příjmu zpráv a režimu spánku (viz Obr. 9)[24]



Obr. 8: Napájení rádiové části.

Při napájení sensorového uzlu se využívá nelineární vybíjecí charakteristika, kdy uzel čerpá energii po impulsech, tedy vybíjení není konstantní.

Napájení prvků se skládá z několika módů, které v závislosti na neaktivním vysílači (přijímači) sníží přes napěťový regulátor odběr senzoru na minimální hranici. U zdroje napájení je velmi důležité co nejmenší procento samovybíjení. Jelikož žádný z akumulátorů nevydrží požadovanou dobu, skládají se zdroje z více článků, kdy je např. sensorový uzel napájen nejdříve určitou dobu z prvního článku, poté přejde na napájení z článku druhého apod. Jako alternativní zdroje energie slouží zdroje z okolního prostředí. Mezi nejpoužívanější patří využívání solární energie a energie vibračních dějů. Výčet nejpoužívanějších typů baterií a jejich parametry je v tabulce níže. [25]

Tab. 3: Typy baterií a jejich parametry [25]

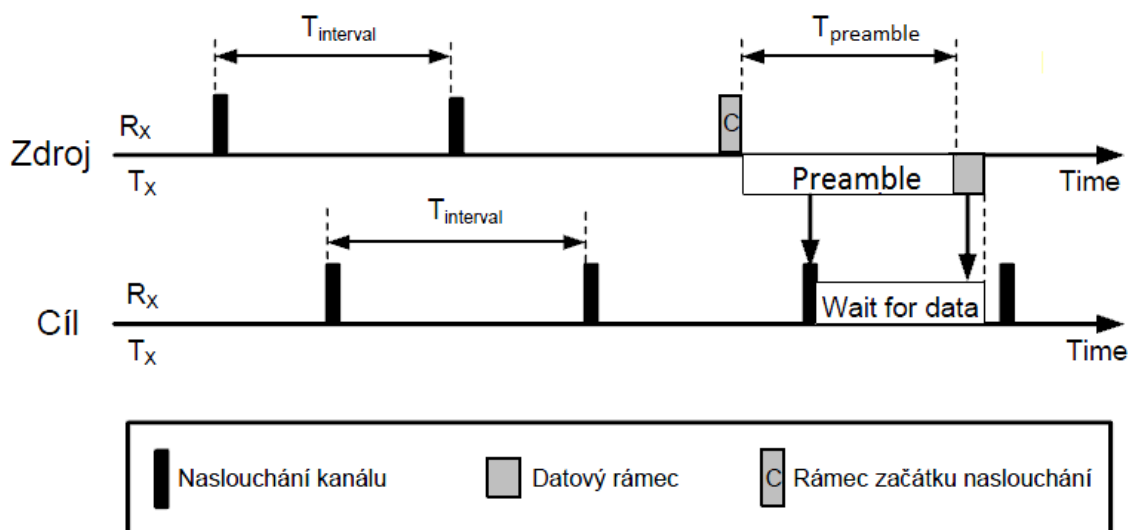
Parametr	Typ akumulátoru				
	Alkalické baterie	Li-Ion	Li-Pol	Ni-Cd	Ni-Mh
Jmenovité napětí [V]	1,5	3,6	3,6	1,2	1,2
Kapacita [mAh]	2400	5000	5000	800	3600
Počet cyklů (vybití-nabití)	1	1000	1000	500	500
Min. hodnota napětí na článek	-	2,8	2,8	0,8	0,8
Samovybíjení (za 1 měsíc)	< 10 %	10%	10%	30%	30%
Paměťový efekt	ne	ne	ne	ano	minimální

3.6.1.2 Na linkové vrstvě

Pro dosažení nízké energetické náročnosti ve WSN sítích jsou jedním z hlavních mechanismů protokoly se synchronním nebo asynchronním režimem. Koncový senzorový uzel může být buď v aktivním režimu, anebo v režimu spánku. Primárním parametrem charakterizujícím jednotlivé stavy je energie spotřebovaná během režimu spánku a aktivního režimu, doba spánku a rychlost probuzení z režimu spánku. Vzhledem k regulaci odběru proudu, řeší vývojáři komunikačních protokolů pro síť WSN, jak dosáhnout vysoké propustnosti a zároveň nízkého zpoždění a co nejmenší energetické náročnosti v aktivním a spánkovém režimu senzorů. Řešení poskytuje vhodné zvolení typu MAC protokolu.

MAC protokoly s asynchronním pracovním cyklem jsou založeny na mechanismu nízko-energetického odposlechu kanálu LPL (Low Power Listening). Uzly měří obsazení kanálu pro přenos (viz Obr. 10). Přenosům předchází preamble (T_{preamble}), který je delší než doba zjišťování obsazenosti kanálu (T_{interval}). Preamble tedy funguje jako jakýsi budicí signál, který uzly probudí do aktivního režimu. V aktivním režimu musí uzel začít posílat data dříve, než bude kanál obsazen [26]. Typy protokolů s asynchronním cyklem:

- B-MAC (Berkeley-MAC) protokol
- Z-MAC protokol
- X-MAC protokol
- WiseMAC protokol



Obr. 10: Asynchronní pracovní režim. [26]

Asynchronní protokoly jsou poměrně jednoduché a vyžadují malé množství paměti v porovnání se synchronními protokoly. Nevýhodou je ovšem poměrně časté naslouchání kanálu bez přenosu dat a s tím spojená nízká energetická účinnost. Asynchronní protokoly jsou vhodné pro WSN sítě s malými přenosovými rychlostmi. Další výhodou je možnost přizpůsobení se dynamickým podmínkám přenosu v síti [5][26].

MAC protokoly se synchronním pracovním cyklem využívají plánování stavu vysílačů a přijímačů, tak aby byl zajištěn pravidelný přenos dat (T_{aktiv} - doba aktivního režimu). Po odvyšlání potřebných dat přechází senzorový uzel opět do režimu spánku (T_{sleep}) umožňující úsporu energie. Aktivní režim a režim spánku se opakují v pravidelných intervalech ($T_{\text{wakeup_period}}$), jak je znázorněno na Obr. 11. Typy protokolů se synchronním režimem:

- S-MAC (Sensor-MAC) protokol

Tab. 5: Srovnání MAC protokolů (asynchronních) [26]

	Synchronní protokoly		
	T-MAC	S-MAC	D-MAC
Počet kanálů	1	1	1
Zabránění neúčinného naslouchání	Periodický režim spánku	Periodický režim spánku	Periodický režim spánku
Topologie	Mesh	Mesh	Mesh
Přístupová metoda	CSMA	CSMA	CSMA
Synchronizace	NE	ANO	NE
Přínos	Režim Aktivní/Spánek	Adaptivní pracovní cyklus	Změny režimu Aktivní/Spánek

4 KAPITOLA

POPIS PROBLÉMU A SPECIFIKACE CÍLE

V této práci bylo hlavním úkolem podrobně popsat vlastnosti, charakter a použití bezdrátových sensorových sítí. Dále pak zhodnotit možnosti zabezpečení perimetru a střežení prostoru. A na základě získaných informací navrhnout a sestavit sensorový uzel pro bezdrátovou sensorovou síť, který bude schopen komunikovat přes síťového koordinátora se sousedními uzly a dohromady tak pomocí tzv. sensorového vidění zabezpečit zvolený perimetr. Jelikož se jedná o bezdrátové sensorové uzly bez možnosti trvalého napájení, je zde kladen velký důraz na energetickou náročnost použitých sensorů v koncových sensorových uzlech.

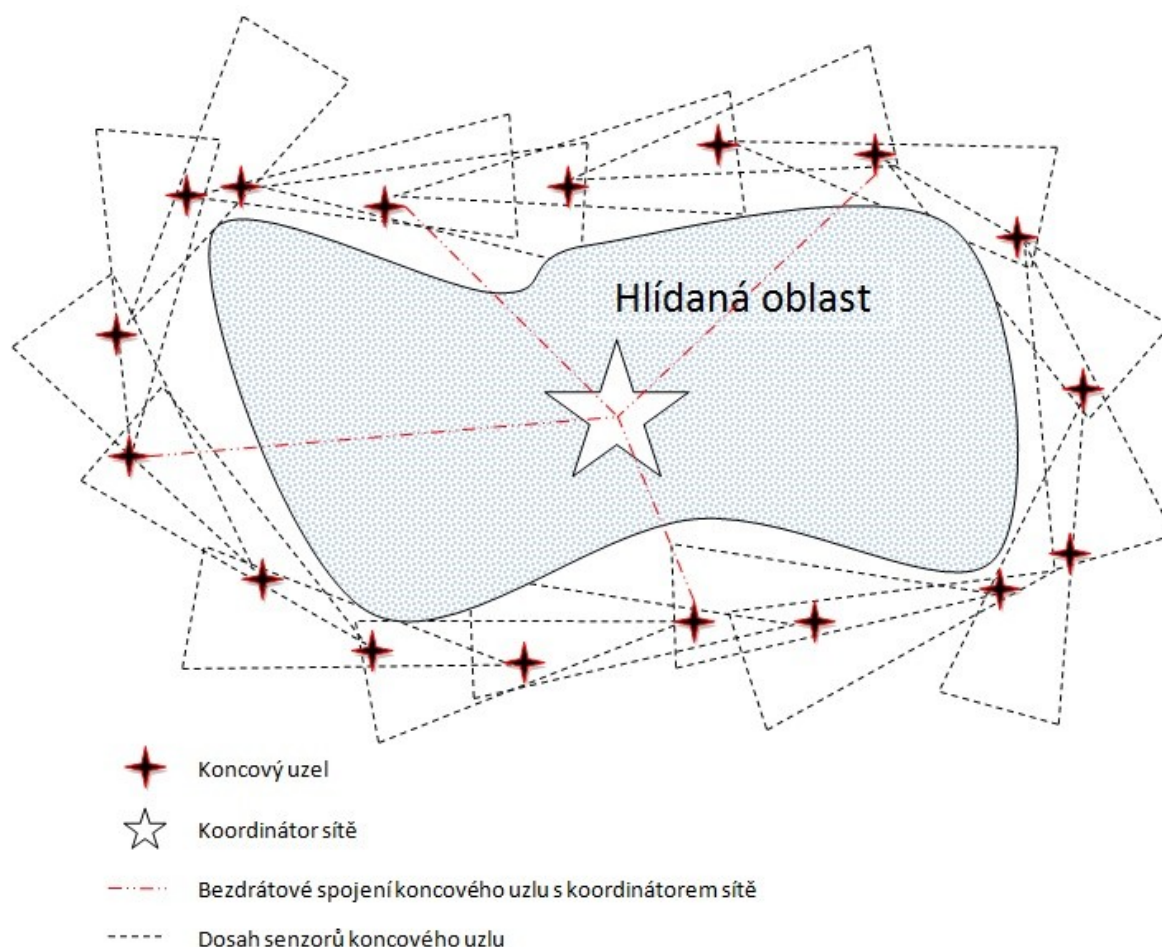
5 KAPITOLA

NÁVRH ŘEŠENÍ

Cílem této kapitoly je seznámení s jednotlivými senzory a principy jejich funkčnosti. Na základě takto získaných zkušeností výběr nejvhodnější kombinace pro řešení daného problému. A dále pak nástin řešení a rozmístění sensorových uzlů v prostoru.

Zabezpečení perimetru pomocí sensorových sítí bude řešeno přes několik koncových sensorových uzlů a jednoho koordinátora sítě v uspořádání do hvězdicové topologie podle Obr. 12. Rozmístění je uspořádáno tak, aby každý uzel viděl na dva následující uzly, tím je dosaženo redundance koncových uzlů. Tedy když uzel přestane pracovat a nebo jej někdo poškodí, systém by měl zůstat stále provozuschopný. Za určitých podmínek může odpadnout až 50 % koncových uzlů, aniž by to ohrozilo funkčnost systému, ale to pouze v případě že nepřestanou pracovat dvě po sobě následující zařízení. Vzdálenosti mezi jednotlivými koncovými uzly se nepředpokládá větší jak 5 m.

Senzorové uzly mohou být díky zvolené hvězdicové topologii ve většině svého provozního času v režimu spánku, protože přes ně nebude směřován žádný provoz od jiného uzlu v síti směrem ke koordinátorovi sítě. Při přiblížení se narušitele k zabezpečenému perimetru se nejbližší sensorové uzly probudí z režimu spánku a budou provádět další měření a zjišťování polohy narušitele a jím překročení střeženého prostoru.



Obr. 12: Návrh zabezpečení, topologie hvězda

5.1 Analýza detektorů

Na trhu je v současnosti nepřehledné množství detektorů a detekčních systémů určených přímo pro perimetrickou ochranu. Zde jsou popsány jen nejpoužívanější. Pro každou konkrétní aplikaci je vhodný jiný detekční princip. Z tohoto důvodu budou uvedeny obecné charakteristiky jednotlivých typů detektorů. Dále bude popsána fyzikální podstata, použití a faktory způsobující falešné poplasy. Popis bude věnován zejména optickým závorám, pasivním infračerveným detektorům (PIR), ultrazvukovým snímačům a otřesovým čidlům.

5.1.1 Rozdělení detektorů z fyzikálního principu

Senzory lze rozdělit podle několika kategorií: podle viditelnosti senzoru

pachatelem, podle tvaru snímací charakteristiky a podle fyzikálního principu činnosti. Podle hlediska vyzařování energie lze senzory dělit na:

- Aktivní – do prostoru vyzařují signál a tím si vytváří detekční prostor. Při narušení detekční zóny osobou dojde ke změně prostředí. Jejich nevýhodou je možnost zjištění přítomnosti takového typu senzoru narušitelem. A dále zde mohou vznikat tzv. mrtvé zóny, tedy prostory kde pachatel není odhalen.
- Pasivní – tyto detektory do prostoru nevyzařují žádný signál, pouze snímají fyzikální změny prostředí ve snímaném prostoru, způsobené při narušení prostoru. Díky tomu, že nevyzařují žádnou energii, jsou velmi obtížně zjistitelné a další jejich výhodou je i malá energetická spotřeba. [13]

5.1.2 Optická závora

Při zabezpečení daného objektu je zejména potřeba zabezpečit obvod pozemku. To znamená, že je třeba použití liniového detektoru. Jedním z takovýchto liniových detektorů je i optická závora. Jedná se o aktivní detektor. Optické závory pracují pokaždé v páru, tedy obsahují vysílač a v přímé linii naproti němu je umístěn přijímač. Vysílač vysílá signál ve formě svazku světelného záření, ať už ve viditelném či infračerveném spektru (IR), směrem k protilehlému přijímači, a tak vytváří hlídanou linii. Počet paprsků mezi vysílačem a přijímačem může být různý. Při použití technologie s velkým množstvím paprsků dojde k vytvoření husté sítě a pro pachatele je velmi obtížné tuto síť překonat. Přijímač v pravidelných intervalech kontroluje zdali došlo k přijetí paprsku a data předává řídicí jednotce, kterou řídí mikroprocesor. Při narušení střežené zóny nežádoucím objektem dojde k přerušení paprsku. Na základě těchto změn a nastavené citlivosti detektor rozhodne, zda se jedná o stav klidu nebo jde o narušení objektu. Typický příklad IR závory je možno vidět na Obr.2.: Zabezpečení skladu. [8]

5.1.2.1 Konstrukce

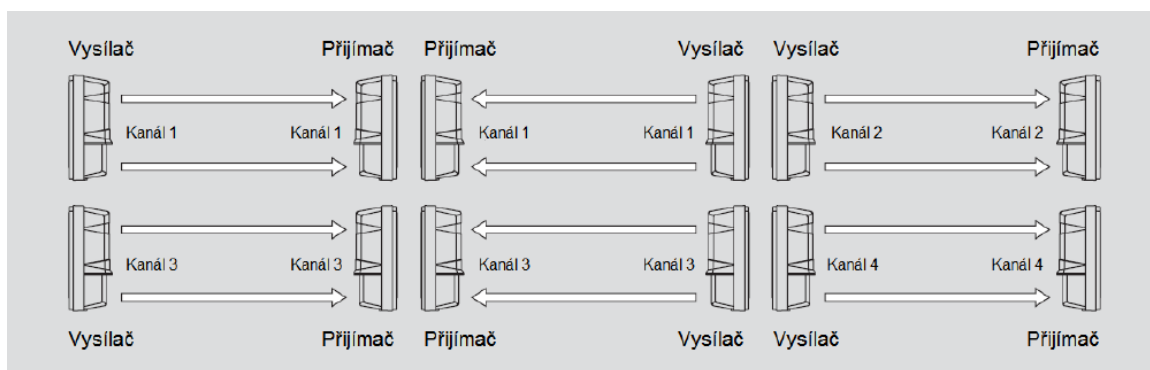
Použití optických závor v extrémních podmínkách znamená, že jsou umístěny

ve venkovním prostředí a jsou vystaveny klimatickým vlivům. Z toho důvodu je nutné zamezit vniknutí prachu a hlavně vody do detektoru. V oblastech, kde mohou působit silné mrazy, je třeba zabránit namrzání vody na čočce závory. Většina detektorů je proti námraze chráněna malou stříškou, ta zabraňuje stékání vody na čočku a následnému vytvoření ledu.

5.1.2.2 Použití

Optické a IR závory a bariéry se nejčastěji používají jako doplněk mechanických zábranných systémů, jako jsou ploty. Tyto detektory se aplikují do objektů, kde potřebujeme střežit linii. Vysílací a přijímací části musí být instalovány tak, aby pracovaly na přímou viditelnost. Proto terén v místě aplikace optické závory musí být rovný a nesmí se v něm nacházet žádné nerovnosti, kterými by mohl pachatel podlézt.

Přijímač i vysílač se umísťuje přímo na sloupky k tomu určené nebo na zeď. Optických závor lze instalovat více do jednoho objektu. Závory lze instalovat v několika uskupeních: v řadě za sebou, nad sebe nebo kombinace těchto dvou možností. U IR závor v tomto případě je nutné nastavit u každé závory jiný modulační kanál Obr. 13. Je to jediný způsob, jak lze realizovat instalace s více IR závorami. U IR závor bývá také problém s nasměrováním vysílače a přijímače, což u optických závor, pracujících ve viditelném spektru nenastává. [8]



Obr. 13: Uskupení IR závor.[8]

5.1.2.3 Falešné poplachy

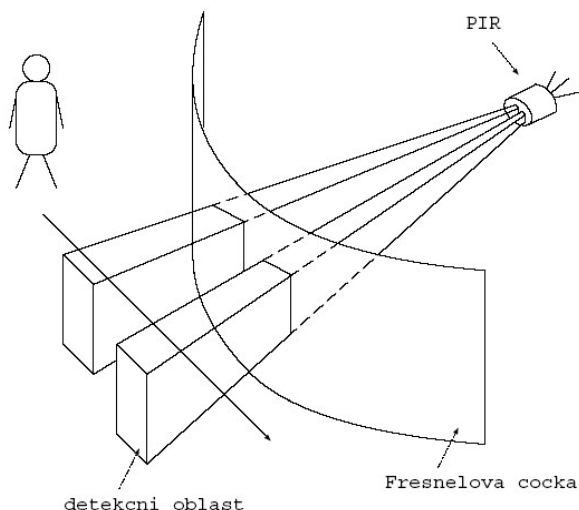
Falešné poplachy u těchto detektorů jsou nejčastěji způsobovány klimatickými vlivy, pohybující se zvířata a u IR závor silnými zdroji infračerveného záření. U laserové

optické závory je minimum falešných poplachů. Způsobem minimalizování falešných poplachů je nutnost přerušení všech paprsků najednou. Dobu přerušení paprsku se pohybuje se přibližně od 50 ms do 500 ms. [9]

5.1.3 Pasivní infračervené detektory

Při zabezpečení objektu není pokaždé možné použití liniových detektorů. Z tohoto důvodu se používají detektory střežící určitý vymezený prostor a mohou být použity jako doplněk pro liniové detektory. Díky tomu může zabezpečit „mrtvé zóny“ liniových detektorů. Jedním z těchto detektorů je pasivní infračervený detektor (PIR). Jak je patrné i z názvu, jedná se o pasivní detektor. PIR detektory nevyzařují žádnou energii, ale snímají dané prostředí. PIR detektor reaguje na změny v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Detekční charakteristika je rozdělena do sekcí. Každá sekce má přesně stanovené rozměry a pozici. Při přechodu pachatele z jedné sekce do druhé dojde k vyhlášení poplachu. [9]

Tyto detektory využívají principu založeném na změně infračerveného záření, jde o tepelné záření. Detektory nezaznamenávají velikost signálu, ale jeho změny. Každé těleso o teplotě mezi $-273\text{ }^{\circ}\text{C}$ a $560\text{ }^{\circ}\text{C}$ vyzařuje infračervené záření. Vlnové délky tohoto záření se pohybují od 760 nm do 1 mm. Teplota lidského těla odpovídá rozmezí vlnových délek 7 – 14 μm . [10]



Obr. 14: Princip PIR detektoru [11]

5.1.3.1 Konstrukce

Mezi nejdůležitější částí PIR detektoru určitě patří pyroelement (Obr. 15.), což je v podstatě součástka podobná fototranzistoru, ale s tím rozdílem, že pyroelement reaguje pouze na infračervené záření. Reaguje pouze na jeho změny a nedokáže detekovat stálou úroveň záření. Tedy pokud narušitel vstoupí do zorného úhlu PIR detektoru, tak pyroelement v určitém místě detekuje odchylku infračerveného záření od normálního stavu pozadí.

Pokud by na pyroelement dopadalo infračervené záření z celého prostoru a do detekční zóny by vstoupil narušitel, vyvolal by pouze jen jednu malou změnu infračerveného záření. Proto pro vylepšení vlastností senzoru se použitím optiky prostor rozdělí do sekcí. Optika bývá realizována pomocí Fresnelových čoček nebo zrcadel. U Fresnelových čoček se jedná o systém využívající lomu paprsků a jsou zhotoveny z plastu. Zrcadla jsou dělena na segmenty a také se vyrábějí z plastu s napařenou kovovou odraznou plochou. Detekční charakteristika vykrytí prostoru je dána geometrií jednotlivých segmentů zrcadla. [12]



Obr. 12: Pyroelement [15]

5.1.3.2 Použití

PIR detektory se umísťují na zdi budov nebo na sloupy. Dosahy těchto detektorů se pohybují v rozmezí od 10 m do 150 m. V perimetrické ochraně se používají detekční charakteristiky typu vějíř s různým úhlem rozevření, popřípadě pro střežení linie typ záclona. Při instalaci se musí brát v potaz směr pohybu pachatele, protože pyroelement je na různé směry jinak citlivý. Při radiálním pohybu směrem k detektoru pachatel musí urazit větší vzdálenost, aby vůbec došlo k detekci. Proto se PIR detektor instaluje tak, aby pravděpodobný pohyb pachatele byl tangenciální. Dále je nutné, aby prostředí bylo

chladnější než teplota lidského těla. Nyní výrobci již tuto nedokonalost řeší teplotními kompenzačními obvody. [13]

5.1.3.3 Falešné poplachy

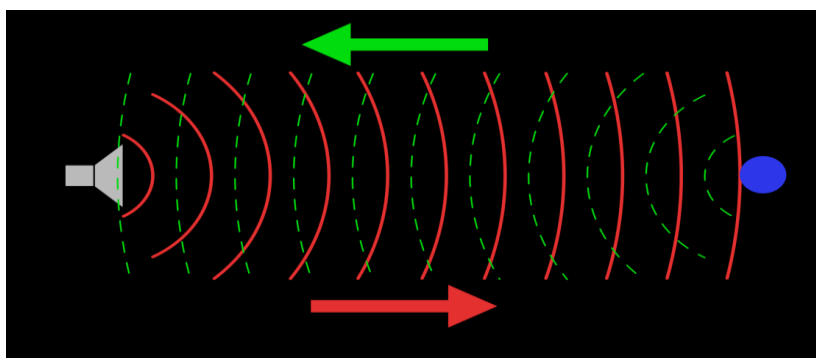
Faktor ovlivňující PIR detektor je především tepelné záření menších zvířat nebo hlodavců, lze je ale omezit vhodnou volbou Fresnelovy čočky a detektor by neměl snímat pohyb přímo u země. Další faktory ovlivňující PIR detektory jsou klimatizace, teplovodní potrubí a další zdroje nepravidelného tepelného záření. Falešné poplachy způsobují také reflektory automobilů i sluneční záření, které ohřívá předmět v detekční zóně. Předmět je pak náhle překryt mrakem, rychle se ochladí a teplotní rozdíl mezi pozadím a předmětem se změní. [17]

5.1.4 Ultrazvuková čidla

Ultrazvuková čidla se využívají především pro měření vzdálenosti, ale také mohou být použita jako doplňkový senzor ke zjištění narušení perimetru. Ovšem je vhodné, aby se ve sledovaném prostoru nenacházel žádný objekt.

5.1.4.1 Konstrukce

Tyto senzory využívají principu zvukového vlnění o frekvenci vyšší než 20 kHz, tedy nad pásmem slyšitelným lidským uchem. Generátor vytváří zvukové vlny o vysoké frekvenci. Tyto zvukové vlny se šíří prostorem, a jakmile narazí na překážku, odrazí se zpět k senzoru (Obr. 16.), který je zachytí a následně přidruženými obvody zpracuje. V senzoru je umístěn jak vysílač, tak i přijímač. [17]

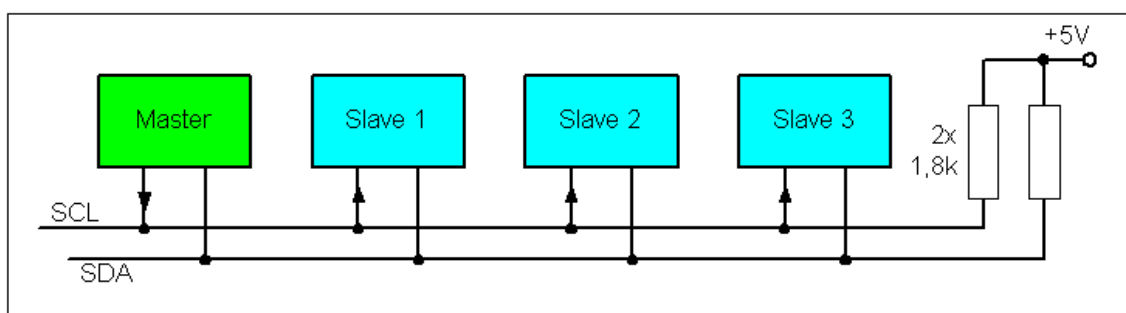


Obr. 16: Princip ultrazvukového senzoru [14]

5.2 Komunikační rozhraní detektorů

5.2.1 Sběrnice I2C

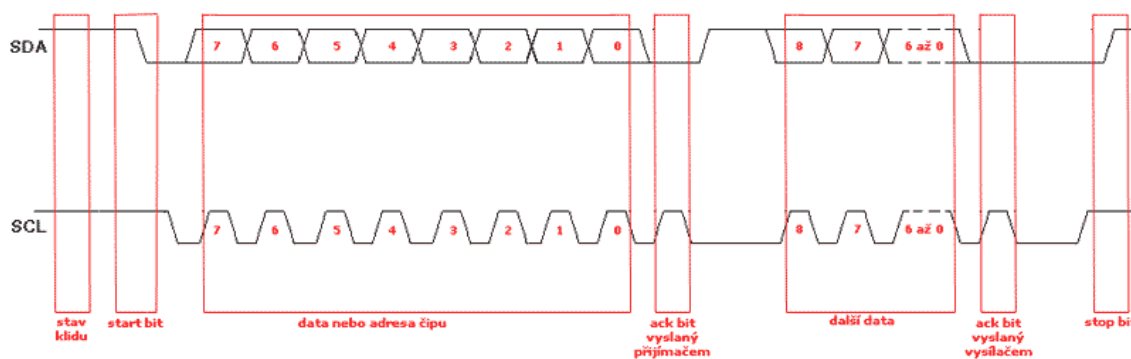
I2C (Inter-Integrated Circuit) je někdy také označována jako TWI (Two Wire Interface). Jedná se o sériovou sběrnici pro komunikaci mezi jednotlivými zařízeními na ni připojenými. Tuto sériovou komunikaci podporuje řada senzorů a integrovaných obvodů (např. RAM a EEPROM paměti, budiče displejů, D/A převodníky atd.). Je fyzicky realizovaná dvěma vodiči: datový (SDA) a hodinový (SCL) vodič. Na jednu sběrnici je možno připojit až 128 (7 bitová adresace), případně 1024 (10 bitová adresace) zařízení v rozšířeném adresním prostoru. Každé zařízení připojené ke stejné sběrnici musí mít individuální adresu. Pokud jsou připojovány například dva integrované obvody s od výrobce nastavenou stejnou adresou, je třeba, pokud je to možné, tuto adresu předem u jednoho z nich změnit. Ukázka zapojení sběrnice je na Obr.: 17. Připojená zařízení se rozlišují na dva typy Master a Slave. Zařízení Master bývá většinou pouze jedno, řídí komunikaci a generuje hodinový signál na SCL. [5]



Obr. 17: Princip I2C sběrnice[5]

V klidovém stavu jsou na sběrnici úrovně logické 1 zajištěné připojenými pull-up rezistory. Každý přenos dat zahajuje zařízení master vysláním start bitu v úrovni logické 0 na vodiči SDA při stále v úrovni logické 1 na vodiči SCL. Se začátkem hodinových impulzů následuje vysílání sedmi nebo deseti bitů adresy příjemce spolu s R/W bitem, který indikuje požadovanou operaci (zápis/čtení dat). Další bit ACK vysílá zařízení slave. Úroveň logické 0 potvrzuje správný příjem a připravenost vysílat/přijímat data. Dále jsou po bajtech přenášena data ve směru určeném bitem R/W. Úroveň na SDA se může změnit jen, pokud SCL v úrovni 0. Každý poslaný byte je ze strany přijímače

(slave) potvrzován bitem ACK. Po ukončení přenosu je vyslán stop bit a oba vodiče uvedeny do klidového stavu. Na Obr. 17 je znázorněn časový průběh komunikace na sběrnici s adresami o délce 7 bitů. [5]



Obr. 18: Ukázka odesílání dat[27]

Standardní frekvence hodinového signálu SCL je 100 kHz, pro Fast Mode 400 kHz a High Speed Mode až 3.4 MHz. Na sběrnici v jednom okamžiku vysílá pouze jedno zařízení, tedy I2C neumožňuje duplexní přenos. Každá ze stanic může zahájit vysílání jen tehdy, je-li sběrnice v klidovém stavu. Používá se metoda s detekcí kolize, vysílač při vysílání kontroluje stav SDA a porovná s odeslanými bity. Je-li zjištěn rozdíl mezi očekávaným a skutečným stavem linky SDA, je indikována kolize.[5]

5.2.2 Rozhraní SPI

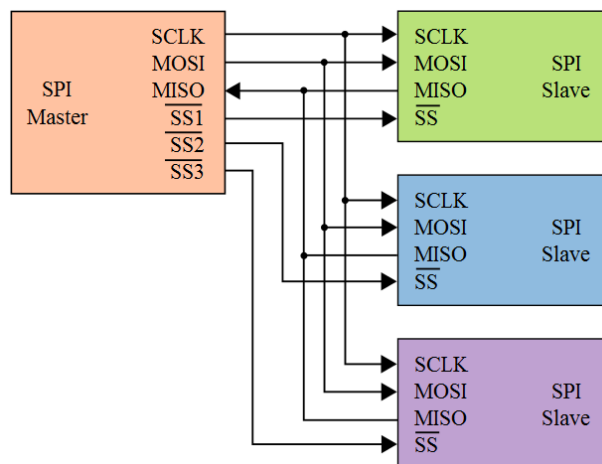
SPI (Serial Peripheral Interface) je sériové periferní rozhraní, které se používá pro komunikaci mezi řídicím mikroprocesorem a ostatními obvody (např. EEPROM, A/D převodníky, displeji apod.). Komunikace je realizována pomocí společné sběrnice, k níž je možno připojit teoreticky libovolný počet zařízení. Zařízení jsou rozdělena na:

Master - řídí komunikaci pomocí hodinového signálu a určuje, které zařízením na sběrnici s ním bude komunikovat. Pomocí vývodu SS (Slave Select) nebo CS (Chip Select).

Slave – pokud je pomocí SS/CS aktivován vysílá data podle hodinového signálu.

Sběrnice je fyzicky realizována dvěma datovými vodiči MISO (Master Input Slave Output), MOSI (Master Output Slave Input), a vodičem pro hodinové impulzy SCLK (Synchronous Clock). V případě, že je připojeno více než jedno Slave zařízení, je třeba

použít adresaci. Ta se provádí pomocí zvláštních vodičů připojených k pinům SS nebo CS (Obr.: 19). Zařízení je aktivováno signálem logické 0. Délka vyslaných dat je buď jeden nebo dva bajty (8/16 bitů).[5]



Obr. 19: Princip sběrnice SPI. [28]

5.3 Výběr detektorů

Jako platformu pro senzorové uzly jsou k dispozici zapůjčené školou (FEKT, VUT Brno) dva moduly eRFnode-2TNP2 sloužící jako koncové zařízení a jeden eRFnode-2TNP2 který bude pracovat jako koordinátor sítě. Tyto moduly obsahují několik vstupně výstupních portů a proto je k nim možno připojit bezpočet senzorů. Sensory mohou s uzlem komunikovat jak přes ADC převodníky pro analogové senzory, tak i po sběrnici I2C.

5.3.1 PIR smd modul 172500



Obr. 20: PIR smd modul 172500 [15]

Parametry PIR modulu:

Tab. 6: Parametry PIR senzoru [15]

Dosah	12m
Napájecí napětí	3-12V
Proudový odběr při aktivním výstupu	1,4mA
Proudový odběr při neaktivním výstupu	1mA
Úhel otevření	120°

Zvolený typ má velice nízkou spotřebu 1 mA při klidovém provozu, což splňuje požadavky sensorové sítě. Dále výstup senzoru je digitální, tedy při narušení prostoru je výstup v logické 1 a v klidovém stavu v logické 0. Existují senzory s ještě nižší spotřebou elektrické energie, ty ale nedisponují potřebným dosahem pro překrývání sensorových uzlů v případě jeho výpadku.[15]

5.3.2 Ultrazvukový senzor SRF 08

Ultrazvukový senzor má větší spotřebu elektrické energie než PIR senzor (viz Tab. 7), ale také se nepředpokládá jeho stálý provoz. Senzor začne s měřením v okamžiku, kdy PIR senzor zachytí přítomnost cizí osoby a vyloučí tak vznik možné chyby. Senzor bude s koncovým zařízením komunikovat po I2C sběrnici. [16]

Tab. 7: Parametry ultrazvukového senzoru [16]

Dosah	6m
Napájecí napětí	5V
Proudový odběr při měření	15mA
Proudový odběr v klidovém stavu	3mA
Úhel otevření	55°



Obr. 21:SRF08 [19]

5.3.3 Optická závora

Optická závora bude použita jako další ochrana a snížení tak počtů planých poplachů, způsobených například osobou, která vstoupí do zorných polí senzorů, ale ještě nepřekročí stanovenou hranici perimetru. Bude použita laserová optická závora díky lepšímu nasměrování dopadajícího paprsku na senzor osvětlení. Díky tomu, že laser bude aktivní pouze po několik sekund, odpadá potřeba jeho chlazení. Zapojení se skládá ze dvou částí, z vysílače a z přijímače umístěného na tomtéž koncovém zařízení a odrazné plochy na sousedním koncovém uzlu. Jako přijímač optické závory bude použito senzoru osvětlení ISL29020IROZ-T7 integrovaného do modulu koncového senzorového uzlu deRFnode-2TNP2, který komunikuje po I2C sběrnici. Parametry senzoru osvětlení jsou uvedeny v Tab. 8.

Tab. 8: Parametry optické závory [18][29]

	Senzor osvětlení	Laserový modul
Rozsah	0,015 - 64000 lux	-
Napájecí napětí	2,25 - 3,6 V	5V
Proudový odběr při měření	65 μ A	35mA
Proudový odběr při režimu spánku	0,5 μ A	-

5.3.4 Akcelerometr BMA150

V zabezpečení samotného koncového zařízení je zvažováno použití akcelerometru, kdy tento senzor je schopen zachytit vibrace okolo daného uzlu. Jedná se o senzor zrychlení, který je schopen změřit vibrace ve čtyřech citlivostních rozsazích, nejnižší je 800mV/g . Vlastnosti senzoru jsou popsány v Tab. 9.

Tab. 9: Parametry BMA150 [20]

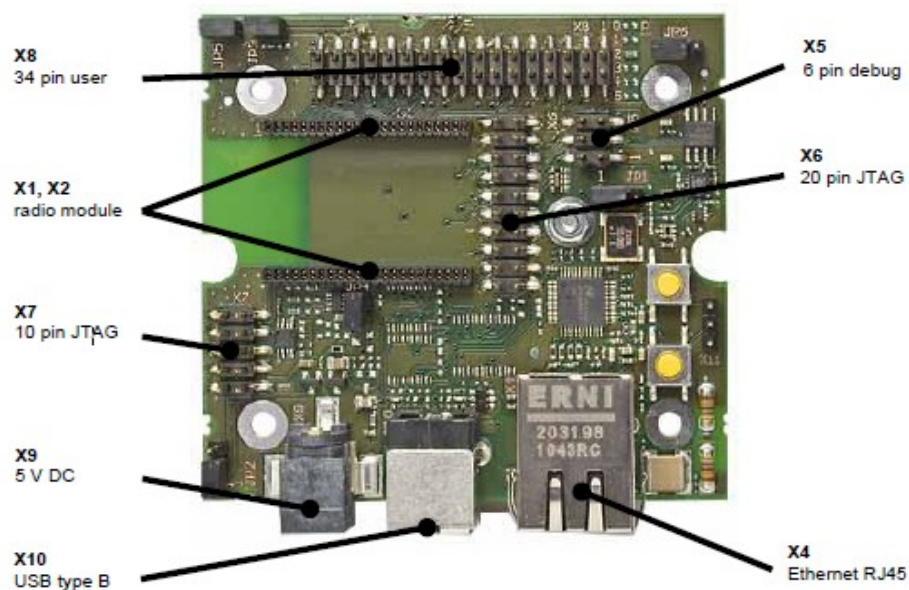
Rozsahy	1,5g/2g/4g/6g
Citlivost	800mV/g při 1,5g
Napájecí napětí	2,2-3,6V
Proudový odběr při měření	500uA
Proudový odběr ve sleep módu	3uA

5.4 Návrh koncového zařízení

Koncové zařízení je tvořeno bezdrátovým senzorovým uzlem deRFnode-2TNP2 od společnosti Dresden Elektornik. Tento senzorový uzel je osazen mikrokontrolerem ATmega 128RFA1, který se stará o komunikaci s bezdrátovým modulem, vysílajícím na frekvenci 2,4 GHz, a periferiemi. Komunikace mezi jednotlivými moduly je možná na vzdálenost 100 až 200 m s přenosovou rychlostí 250 kbit/s. Modul podporuje protokol 6LoWPAN a byl navržen pro WSN sítě. Jedná se v podstatě o vývojový kit, který obsahuje řadu doplňků jako jsou:

- USB a Ethernet (pouze koordinátor sítě) rozhraní
- JTAG rozhraní
- Senzory zrychlení, osvětlení a teploty
- Paměť o velikosti 4Mbit
- Dvě tlačítka a tři LED diody
- GPIO piny vyvedené na 34 pinovou lištu X8

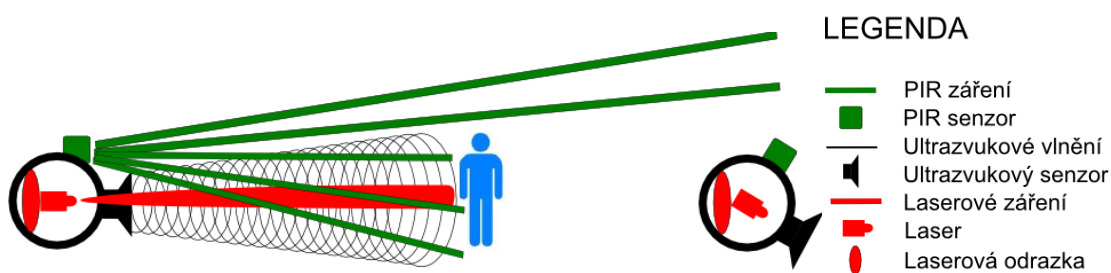
Napájet tento kit je možné buď 5V přes DC vstup nebo přes rozhraní USB a při maximálním zatížení nepřesahuje spotřebu 50 mA. Běžná hodnota proudového odběru se pohybuje kolem 15 – 50 mA a při vypnutém vysílači je odběr 2 uA.[21]



Obr. 22: deRFgateway-1TNP2 [21]

5.4.1 Popis a schéma koncového zařízení

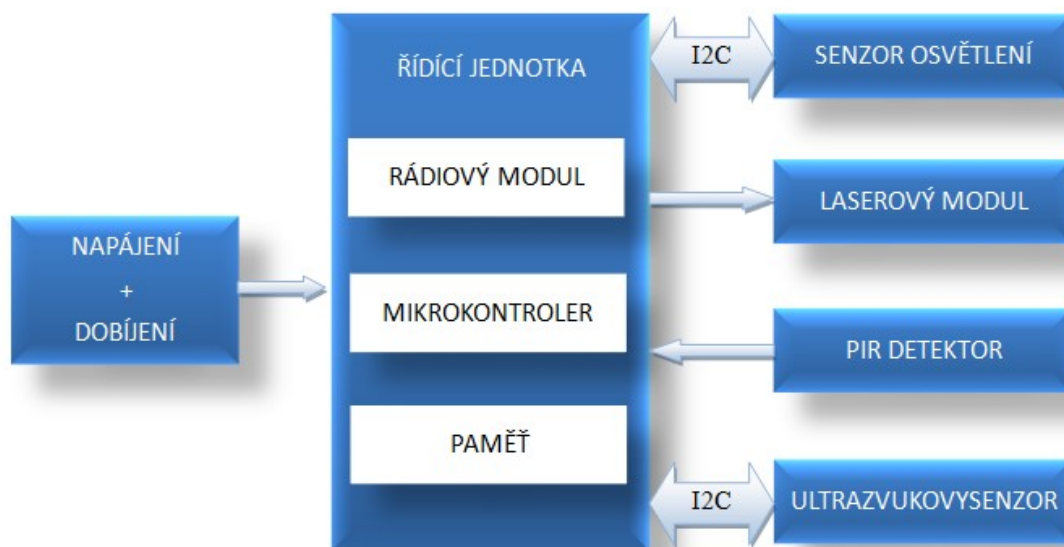
Senzorový uzel tvořený kitem deRFnode-2TNP2 a vybranými typy senzorů je vidět na Obr. 23 a 24, kde je i naznačeno překročení perimetru mezi dvěma koncovými uzly. Jednotlivé senzory jsou osazeny na desce plošných spojů s uzlem spojené přes vstupně výstupní porty vyvedené na pinovou lištu X8. Dva koncové uzly jsou od sebe vzdálené maximálně 5 m na přímou viditelnost. [22]



Obr. 23: Rozmístění dvou senzorových uzlů

Základním blokem koncového senzorového uzlu je řídicí jednotka, která řídí a zpracovává hodnoty naměřené pomocí různých druhů senzorů. Senzory jsou celkem zvoleny tři a to každý na rozdílném principu činnosti. Díky tomu je zajištěna eliminace vzniku planých poplachů a senzorový uzel reaguje pouze na podněty narušení

perimetru. Samozřejmě správnou funkčnost ovlivňuje i umístění sensorových uzlů, kde se předpokládá poloha minimálně 50 cm od povrchu země a přímá viditelnost na sousední prvky.



Obr. 24: Blokové schéma zapojení koncového uzlu se senzory

Na každém koncovém uzlu jsou umístěny všechny tři typy senzorů a to PIR čidlo, ultrazvukový senzor a laserová optická závora. PIR čidlo je stále napájené a bez přestání vyhodnocuje vymezený prostor kolem sebe. Neustálé napájení a měření není kritické díky jeho nízké spotřebě, při neaktivním výstupu (Tab. 16), jenž zatěžuje baterie minimálně. Narušení prostoru jako první zaznamená PIR čidlo a probere tak z režimu spánku pouze onen koncový uzel a zbytek uzlů svůj stav nemění (viz topologie sítě Obr. 12). Tudíž celá odpovědnost za probuzení uzlu spadá právě na PIR čidlo. Uspávání systému bude záviset opět na PIR čidlu a na aktivitě ostatních senzorů. Pokud PIR čidlo zachytí pohyb, aktivuje se ultrazvukový senzor, který bude po dobu 10 s provádět měření. Pokud ultrazvukový senzor nezaznamená změnu oproti výchozímu stavu, koncový sensorový uzel se uspí. Ovšem je-li změna detekována, sepne se optická závora opět po dobu 10 s a čeká se na její přerušení, pokud k přerušení optické závory nedojde, sensorový uzel se uspí. Když všechny tři senzory zaznamenají narušení perimetru je odeslána zpráva koordinátorovi sítě o poplachu. Tímto je zabráněno zbytečnému vypínání a zapínání buňky, pokud by se objekt, jenž aktivaci vyvolal, na okamžik zastavil.

Podle zadání stačí vyhodnotit pouze došlo-li k narušení perimetru, ovšem díky zvolené topologii a systému probouzení prvků v síti lze podle jeho adresy určit i místo a přesnou polohu objektu.

5.4.2 Energetická spotřeba koncového zařízení

Navrhovaný sensorový uzel bude ve většině času v režimu spánku, ovšem ale spotřeba elektrické energie závisí na provozu a počtu narušení prostoru a na vzdálenosti koncového uzlu od koordinátora sítě. Jak již bylo výše zmíněno největší energetickou spotřebu bude vykazovat sbírání dat, tedy zjišťování narušení prostoru. Proudový odběr při režimu spánku je přibližně 2 mA a při narušení prostoru, tedy aktivaci všech senzorů a odesílání dat by se spotřeba neměla dostat přes 100 mA. O napájení koncového sensorového uzlu se starají tři tužkové akumulátory (AA) o celkovém napájecím napětí 3,6 V při použití tytu Ni-Mh.

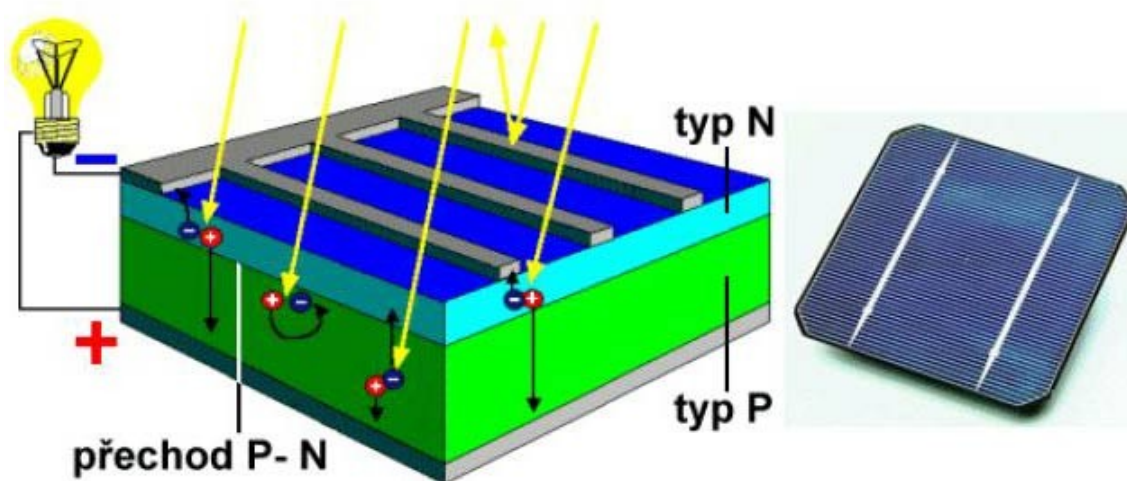
Při volbě vhodných typů akumulátorů bude nejdůležitějším parametrem samovybíjení. Tento parametr mají nejlepší alkalické baterie, ty ovšem neumožňují dobíjení. Zbývají tedy pouze akumulátory na bázi niklu, jelikož Li-Ion ani Li-Pol nelze použít díky vestavěnému pouzdru na akumulátory velikosti AA. Ty ovšem trpí poměrně velkým samovybíjením a to poklesem energie až o 30 % za měsíc, proto je nutno zvolit dobíjení akumulátorů pomocí alternativních zdrojů energie.

U nabíjení Ni-MH akumulátorů je nutno věnovat zvláštní pozornost k přebíjení článků (nabíjení článků i po dosažení stavu plného nabití), neboť vede k nevratným negativním změnám parametrů. Před nabíjením je důležitá stabilizovaná teplota akumulátoru. Nabíjení akumulátorů s teplotou pod 15°C a nad 30°C se projeví v dalším cyklu nabíjení poklesem jeho kapacity.

5.4.2.1 Alternativní zdroj energie

Jelikož koncový sensorový uzel je bezdrátový nepředpokládá se tedy, že dobíjení akumulátorů bude možné pomocí elektrické sítě, proto je nutné zvolit jiný způsob získávání energie. Nabízí se hned několik možností odkud tuto energii získat, jako nejpoužitelnější jsou zde uvedeny tři příklady:

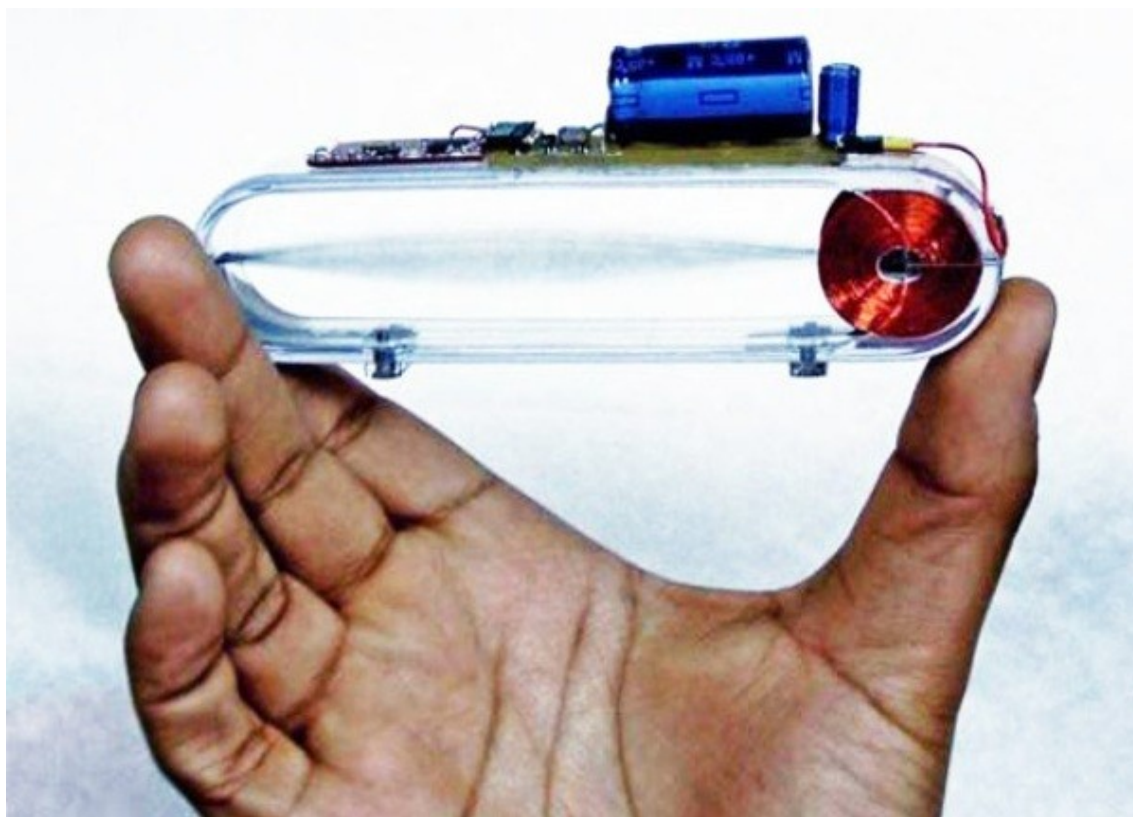
- **Fotovoltaický článek** - využívá přímé přeměny světelné energie na elektrickou v polovodičovém prvku označovaném jako fotovoltaický (solární) článek. Fotovoltaický článek je v podstatě dioda alespoň s jedním PN přechodem. V ozářeném článku jsou generovány elektricky nabitě částice (páry elektron – díra). Elektrony a díry jsou separovány vnitřním elektrickým polem PN přechodu a rozdělení jejich náboje má za následek napěťový rozdíl mezi horním (-) a spodním (+) kontaktem fotovoltaického článku. Vnější obvodem zapojeným mezi oba kontakty potom protéká stejnosměrný elektrický proud, který je přímo úměrný ploše solárního článku a intenzitě dopadajícího slunečního záření. Napětí jednoho článku se pohybuje přibližně kolem 0,5 V, proto se sériovým či sério-paralelním propojením budují sestavy pro jmenovité provozní napětí 12 nebo 24 V, které jsou hermeticky uzavřeny ve struktuře krycích materiálů do výsledného solárního panelu.



Obr. 24: Fotovoltaický článek [30]

- **Windbelt-** zařízení skládající se z pásu (windbeltu), silného magnetu a cívek. K výrobě elektrické energie využívá windbelt větru, který proudí kolem napnutého plastového pásu. Takto napnutý pásek vlivem proudícího vzduchu začne rezonovat. Na konci pásu jsou uchyceny magnety, které kmitají určitou frekvencí. Frekvence kmitání se pohybuje se od 50 do 100 Hz a je závislá na délce pásu a síle větru. Kolem pásu jsou uchyceny cívky, mezi nimiž kmitá

magnet. Systém windbelt využívá elektromagnetické indukce, tedy vlivem pohyblivého magnetického pole, které vyvolávají permanentní magnety, se do cívek indukuje střídavé napětí. Účinnost zařízení se liší podle délky pásu a síly větru. Nejúčinnější prototypy jsou schopny výkonu blížícímu se až 50W.



Obr. 25: Windbelt [31]

6 KAPITOLA

KONSTRUKCE

Ke stávajícímu bezdrátovému sensorovému uzlu deRFnode je navržnuta pouze deska s osazenými typy sensorů. Kompletní bezdrátový sensorový uzel je vyfocen na Obr. 26.

6.1 Popis návrhu zapojení

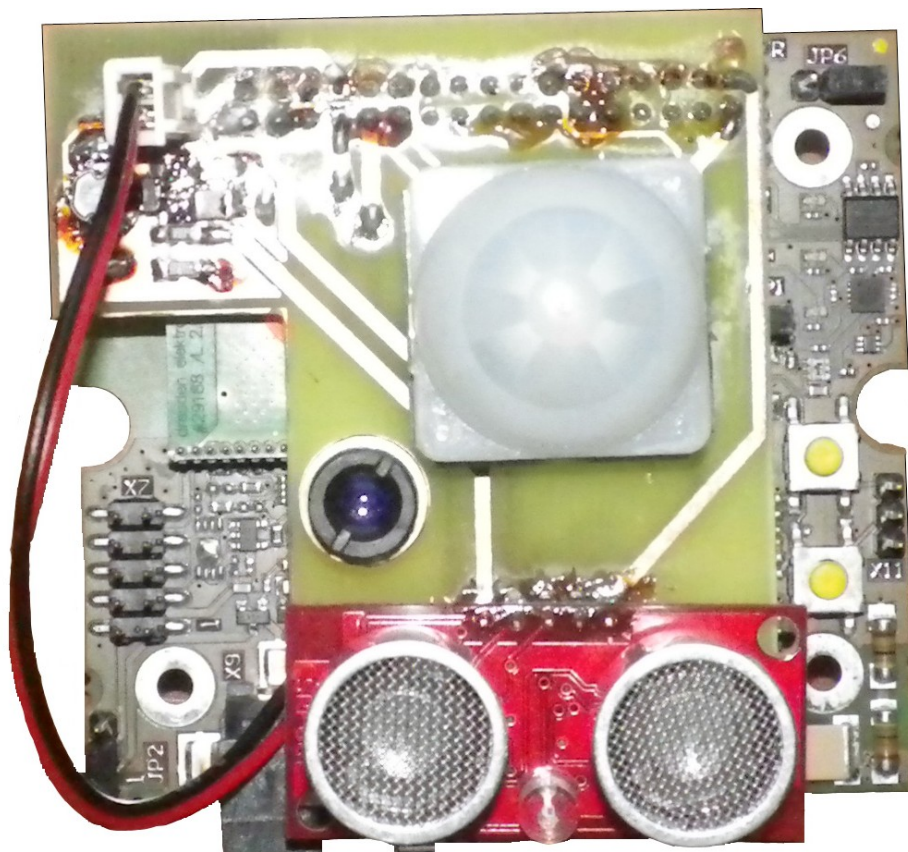
Navržená deska propojuje PIR čidlo, laserový modul a ultrazvukový senzor s uživatelským rozhranním X8 dle[21].

PIR čidlo nebylo nutno nijak upravovat, podle manuálu dodávaného výrobcem lze pomocí pájecích propojek (jumperu) nastavovat citlivost ve čtyřech stupních. Zvoleno je tedy nejvyššího dosahu pomocí propojky J1[15]. Čidlo má dva výstupy, jeden výstup je čistě digitální, kdy při rozpoznání pohybu je vygenerovaná úroveň logické 1 kompatibilní s logikou TTL a CMOS. Druhý výstup je analogový, kde výstupní amplituda závisí na rozdílu záření a provozním napětí. Zde je zvolen digitální výstup označený jako pin 5, který při přechodu do aktivní úrovně probudí pomocí externího přerušování INT4, pin 13 uživatelského rozhraní X8, sensorový uzel z režimu spánku.

Ultrazvukový senzor vzdálenosti SRF08 komunikuje s mikrokontrolérem pomocí sběrnice I2C, jejíž datová linka je připojena na pin 26 a hodinová linka na pin 28 uživatelského rozhraní X8. Senzor vzdálenosti je určen pro napájecí napětí 5V, kdežto sensorový uzel pracuje na napětí pouze 3 až 3,6 V. Zde je využito obvodu MPC1640, což je DC / DC měnič, který zvětšuje provozní napětí uzlu na napětí potřebné k chodu senzoru vzdálenosti. Měnič napětí je zapojen dle katalogového listu [32], kde pomocí zpětné vazby určené rezistory R1 a R2 výstupní napětí, v našem případě 5 V. Proudová spotřeba samotného obvodu je 1 mA, samozřejmě reálná spotřeba je mnohonásobně větší díky spotřebě při převodu na vyšší napětí a proudovému odběru samotného senzoru vzdálenosti.

Optická závora je složena z laserového modulu [18], senzoru osvětlení [29]

a odrazové plochy umístěné na sousedním sensorovém uzlu, mezi kterým zabezpečuje daný prostor. Laserový modul je připojen pomocí vnitřního pull-down rezistoru mikrokontroléru, díky čemuž proudově nezatěžuje jeho výstupní port. Senzor osvětlení komunikuje po stejné I2C sběrnici jako senzor vzdálenosti SRF08.



Obr. 26: Bezdrátový sensorový uzel

6.2 Návrh plošného spoje

Pro návrh desky plošných spojů byl zdroj čerpání informací předmět BKEZ o návrhu DPS, z něhož bylo při návrhu vycházeno. Obrazy DPS zde uvedené nejsou v měřítku 1:1. Při výrobě je vždy třeba používat přímo zdrojové soubory z programu EAGLE, které jsou přiloženy formou přílohy na CD. Vzhledem k nutnosti použití konektorů jak na straně TOP, tak i na straně BOTTOM bylo použito oboustranné prokovené desky plošných spojů. Výkresy plošných spojů a osazovací nákras se nachází v příloze 1. Soubory jsou vytvořeny v programu EAGLE verze 6.1.0. Seznam všech použitých součástek a jejich typové označení je uvedeno v příloze 2.

6.2.1 Technické požadavky na DPS:

- Materiál DPS: FR4
- Tloušťka materiálu: 1,5mm
- Síla mědi: 17 μ m
- Vrtaná DPS: ANO
- Deska je navržena jako oboustranná, s prokovenými otvory bez drátových propojek.
- Nepájivá maska: NE
- Potisk: NE

7 KAPITOLA

FIRMWARE

Tato část je věnována vývoji programu pro mikrokontrolér ATmega128RFA1. Mikrokontrolér byl programován přes rozhraní JTAG pomocí programátoru ATMEL AVRAJTAGICE_MKII. Samotný program pak byl vytvářen v programu AVR Studio 5.1 v programovacím jazyku „AVRGCC“, což je obdoba jazyku „C“.

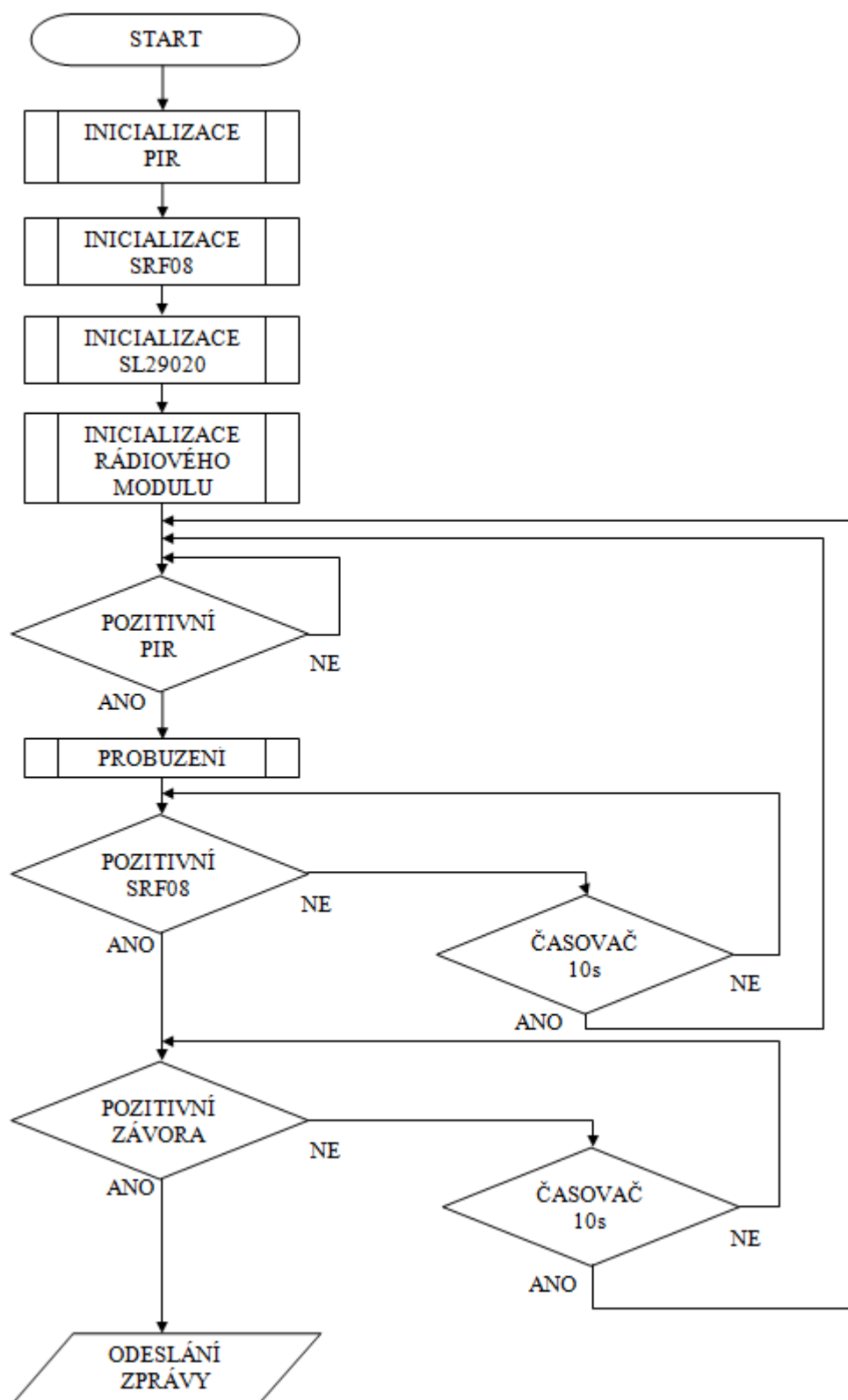
Pro programování mikrokontroléru bylo především využito literatury [19], [20] a skript [5] k předmětu bezdrátové sensorové sítě pana Ing. Milana Šimka, Ph.D. Kódy jsou vytvořeny dva, jeden pro koordinátor sítě a druhý pro koncový bezdrátový uzel.

7.1 Bezdrátový sensorový uzel

Vytvořený kód tvoří samostatný blok, kde probíhají měření jednotlivých senzorů, které pracují automaticky bez nutnosti zásahu uživatele. Při rozšíření sítě o další koncové sensorové uzly je nutné změnit jeho adresu, aby se v síti nenacházela dvě zařízení se stejnou adresou.

Po zapnutí koncového uzlu dojde k celkové inicializaci mikrokontroléru, kdy jsou inicializovány jednotlivé porty, I2C sběrnice, rádiový modul, proměnné programu a připojení do sítě. Vývojový diagram je vidět na Obr. 27.

Na internetu je dostupná řada knihoven, určená pro osmibitové mikrokontroléry. Tyto knihovny jsou v podstatě zdrojové kódy, které umožňují komunikaci podle standardu 802.15.4. Jedná se o předpřipravené kódy pro mikrokontrolér. Většina z nich je šířena pod licencí, která dovoluje jakýkoliv zásah do kódu a tudíž jeho libovolnou modifikaci. Při návrhu analyzátoru byla použita knihovna `µracoli` [33]. Na knihovnu `µracoli` se vztahuje tzv. modifikovaná BSD licence. Tato licence v podstatě říká, že se jedná o volně šiřitelný, open-source, software. Přesné znění licence dostupné na [33]. Knihovna `µracoli` je využito k odesílání dat přes rádiový modul, tedy zprávy obsahující informaci o narušení perimetru. Dále je využito ukázkových příkladů, stažených ze stránek výrobce Dresden Elektronik. [34]

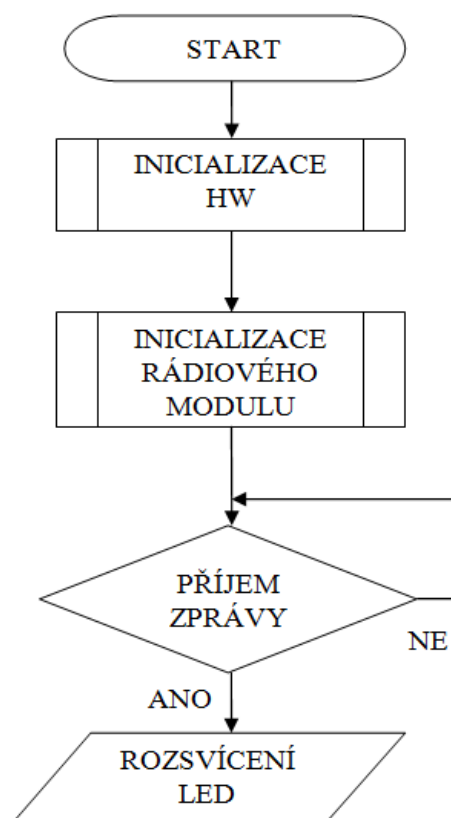


Obr. 27: Vývojový diagram senzorového uzlu

7.2 Koordinátor sítě

Hlavní účel koordinátoru sítě je po zapnutí vytvořit síť, do které se ostatní prvky mohou připojovat. Jakmile je síť vytvořena, přesouvá se ze stavu, ve kterém čeká na příchozí data od koncových prvků. Koordinátor je po celou dobu zapnut a připojen k napájení. Jedná o zařízení typu FFD na rozdíl od bezdrátového senzorového uzlu.

Firmware pro je vytvářen v AVR Studiu 5.1 s využitím nadstavby BitCloud, díky tomu je možno jako koordinátora sítě použít prvek jak s mikrokontrolérem ATmega 128RFA1, tak i ARM7.



Obr. 28: Vývojový diagram koordinátora sítě

8 KAPITOLA

ZÁVĚR

Cílem této diplomové práce bylo teoreticky analyzovat úlohu zabezpečení perimetru v extrémních podmínkách pomocí sensorových sítí. Seznámit se s množstvím výrobcí nabízených senzorů, zhodnotit jejich vlastnosti a vybrat nejlépe odpovídající typy s ohledem na použitelnost v daném prostředí a nízkou spotřebu. Dále je zde pojednáváno o problematice zabezpečení prostoru a o problematice bezdrátových sítí. V následujících kapitolách je podrobný popis návrhu a konstrukce řešení. V navrženém zabezpečovacím systému je zvoleno několik typů senzorů pracujících na odlišných principech a to pro opravdu vysokou spolehlivost a s důrazem na nízkou spotřebu použitých senzorů.

V této práci jsou uvedeny veškeré teoretické informace o vybraných senzorech a použitých prvcích sítě, jako jsou koncová zařízení, směrovače (routery) a koordinátory sítě.

Navržený koncový bezdrátový sensorový uzel, při zaznamenání narušení perimetru střeženého prostoru, vyšle zprávu o tomto narušení svému koordinátorovi sítě, který spustí poplach. Díky hvězdicové topologii, která je zde použita, mohou být zbylé uzly, jež nezaznamenaly žádný pohyb, v režimu spánku a tím šetřit energii. V kapitole pojednávající o energetické spotřebě koncového zařízení, je uvedeno několik způsobů jak dobíjet instalované akumulátory a prodloužit tak životnost koncového uzlu. Topologie a princip rozmístění sensorových uzlů je na obrázku 12, rádiový dosah jednotlivých senzorů ve volném prostředí je maximálně 200 m, díky tomu lze, v ideálním případě, pomocí tohoto návrhu zabezpečit prostor o maximálním průměru 400 m. Pokud by byl požadavek na zabezpečení prostoru většího jak 100 000 m² je nutno zvolit jiné topologie (např. mesh), kdy se perimetrická síť bude skládat i ze zařízení typu router.

LITERATURA

- [1] NATOAKTUAL.CZ. Armáda ukázala jedno z nejhliďanějších míst v zemi. In: *Armáda ukázala jedno z nejhliďanějších míst v zemi* [online]. natoaktual.cz, 2012 [cit. 2012-12-10]. Dostupné z: http://www.natoaktual.cz/armada-ukazala-prisne-strezeny-municni-sklad-fap-na_zpravy.aspx?c=A121129_094824_na_zpravy_m00
- [2] KREIBICH, Ondřej a Jan NEUŽIL. *Bezdrátové senzorové sítě* [online]. Praha: ČVUT v Praze, Fakulta elektrotechnická, 2011/3 [cit. 2012-12-10]. ISSN 110342; 110342. Dostupné z: <http://www.mmspektrum.com/clanek/bezdratove-senzorove-site.html>
- [3] ZHANG, Jeffrey. Wireless Sensor Network (WSN). In: *Wireless Sensor Network (WSN)* [online]. Sydney, 2012 [cit. 2012-12-10]. Dostupné z: <http://zijie.net/research.php>
- [4] Technology - Decentlab: WSN Deployment. *Technology - Decentlab: WSN Deployment* [online]. 2012 [cit. 2012-12-10]. Dostupné z: <http://www.decentlab.com/index.php?id=2>
- [5] ŠIMEK, Milan. *Bezdrátové senzorové sítě*. BRNO, 2012. 163 s. Skripta. VUT Brno.
- [6] et alTHE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Inc. IEEE Computer Society. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. USA: 3 Park Avenue, New York, NY 10016-5997, 2007, 203 s. ISBN 0-7381-5583-7 SH95677. Dostupné z: <http://ieeexplore.ieee.org/>
- [7] et alREILLY TECHNOLOGY CORP. Reilly Technology: What is a Wireless Sensor Network?. *Reilly Technology: What is a Wireless Sensor Network?* [online]. 2011 [cit. 2012-12-10]. Dostupné z: <http://www.reillytechnology.com/home/article/1>
- [8] ADI Global Distribution: ADI - PERIMETR. In: *ADI - PERIMETR* [online]. 2011

- [cit. 2012-12-11]. Dostupné z:
<http://www.adiglobal.cz/iiWWW/cz/produkty150.nsf/wp/index>
- [9] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. S.l.: Cricetus, 2003, 351 s. 3. aktualizované. ISBN 80-902-9382-4.
- [10] MACHÁČEK, Martin. *Encyklopedie fyziky*. 1. vyd. Praha: Mladá fronta, 1999, 408 s. ISBN 80-204-0237-3.
- [11] VOJÁČEK, Antonín. Kontrola místnosti / prostoru GSM PIR čidlem. *Kontrola místnosti / prostoru GSM PIR čidlem* [online]. 2009 [cit. 2012-12-11]. Dostupné z:
<http://automatizace.hw.cz/kontrola-mistnosti-prostoru-gsm-pir-cidlem>
- [12] UHLÁŘ, Jan. *Technická ochrana objektů. II.díl: Elektrické zabezpečovací systémy II*. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-725-1189-0.
- [13] Senba D203S PIR Sensor ,passive human motion detector. *Senba D203S PIR Sensor ,passive human motion detector* [online]. 2012, 4.1.2012 [cit. 2012-12-11]. Dostupné z:
http://www.bombayharbor.com/Product/59726/Senba_D203s_Pir_Sensor.html
- [14] WONG, Kerry D. A Sensitive DIY Ultrasonic Range Sensor. *A Sensitive DIY Ultrasonic Range Sensor* [online]. 2011, 22.1.2012 [cit. 2012-12-11]. Dostupné z:
<http://www.kerrywong.com/2011/01/22/a-sensitive-diy-ultrasonic-range-sensor/>
- [15] PIR senzor SMD Hygrosens 3 - 12 V, 120°, dosah 12 m. *Conrad.cz* [online]. 2012 [cit. 2012-12-11]. Dostupné z: <http://www.conrad.cz/pir-senzor-smd-hygrosens-3-12-v-120-dosah-12-m.k172500>
- [16] SRF08 [115-003]. *Snail Instruments* [online]. 2012 [cit. 2012-12-11]. Dostupné z:
http://shop.snailinstruments.com/index.php?main_page=product_info&cPath=65_7%20%202&products_id=194
- [17] Thefullwiki.org: Ultrasound. *Ultrasound: Ultrasonic range finding* [online]. 2010, 14.1. 2010 [cit. 2012-12-11]. Dostupné z: <http://www.thefullwiki.org/Ultrasound>

- [18] SHAWO HWA INDUSTRIAL CO.,LTD. Datasheet. *650NM LASER MODULE*. Taiwan, 2006, 2 s. Dostupné z: <http://www.gme.cz/dokumentace/758/758-009/dsh.758-009.1.pdf>
- [19] Robot-electronics: SRF08 Ultra sonic range finder. *SRF08 Ultra sonic range finder* [online]. 2010 [cit. 2012-12-11]. Dostupné z: <http://www.robot-electronics.co.uk/html/srf08tech.html>
- [20] FREESCALE SEMICONDUCTOR. Datasheet. *Micromachined Accelerometer: MMA7260Q*. 2006, 8 s. Dostupné z: <http://www.gme.cz/dokumentace/955/955-062/dsh.955-062.1.pdf>
- [21] PIETSCHMANN, Manuel. DRESDEN-ELEKTRONIK. Manual. 6LoWPAN Workshop. 175 s.
- [22] DRESDEN-ELEKTRONIK. User manual. DeRFnode and deRFgateway. 1.2. Dresden-Elektronik, 2012, 79 s. Dostupné z: http://www.dresden-elektronik.de/funktechnik/uploads/media/deRFnode_deRFgateway-BHB-en_10.pdf
- [23] CHIANG, Mu-Huan. Energy Optimization in Wireless Sensor Networks. North Carolina State University, 2007, USA : VDM Verlag Dr. Müller e.K., ISBN 978-3-8364-6132-0
- [24] SHELBY, Zach; BORMANN, Carsten. 6LoWPAN : The wireless embedded internet. Southern Gate, Chichester, United Kingdom : John Wiley & Sons Ltd, 2009. 219 s. ISBN 978-0-470-74799-5.
- [25] BLUEJAY, Michael. Michael Bluejay's.com [online]. 2002 [cit. 2013-05-03]. Household Battery Types Compared (AAA, AA, C, D, and 9V). Dostupné z: <http://michaelbluejay.com/batteries>
- [26] KOHVAKKA, Mikko. Medium Access Control and Hardware Prototype Desings for Low-Energy Wireless Sensor Network. Tampere University of Technology : Tampereen teknillinen yliopisto, 2009. ISBN 978-952-15-2189-B.
- [27] Hw.cz : Teorie a praxe [online]. 19.5.2000 [cit. 2013-05-03]. Stručný popis

sběrnice I²C a její praktické využití k připojení externí eeprom 24LC256 k mikrokontroléru PIC16F877. Dostupné z:
http://www.hw.cz/design/i2c_pic/index.html

- [28] SPI. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 18. 8. 2011 [cit. 2013-05-03]. Dostupné z:
<http://cs.wikipedia.org/wiki/SPI>
- [29] INTERSIL. ISL29020: A Low Power, High Sensitivity, Light-to Digital Sensor With I2C Interface [datasheet]. 2009, 11 s. Dostupné z:
<http://www.intersil.com/content/dam/Intersil/documents/fn65/fn6505.pdf>
- [30] BLUMENTRITT, Pavel. PROTECH GROUP S.R.O. Základní informace o fotovoltaičce: Fotovoltaiický jev [online]. 2013, 22.5.2013 [cit. 2013-05-23]. Dostupné z: <http://www.protech-group.cz/sluzby/stavba-fotovoltaiicke-elektrarny/princip-fotovoltaiiky/>
- [31] PROEFROCK, Philip. Energy: Windbelt: Innovative Generator to Bring Cheap Wind Power to Third World Read more: Windbelt: Innovative Generator to Bring Cheap Wind Power to Third World [online]. 2010 [cit. 2013-05-24]. Dostupné z: <http://inhabitat.com/windbelt-innovative-generator-to-bring-cheap-wind-power-to-third-world/>
- [32] MICROCHIP TECHNOLOGY INC. Datasheet. MCP1640/B/C/D, 2010, 32 s. Dostupné z: http://www.siongboon.com/projects/2005-08-07_lm2576_dc-dc_converter/MCP1640.pdf
- [33] uracoli: The µController Radio Communication Library [online]. 9.4.2013 [cit. 2013-05-24]. Dostupné z: <http://www.nongnu.org/uracoli/index.html>
- [34] DRESDEN ELEKTRONIK. Wireless solutions [online]. 2013 [cit. 2013-05-24]. Dostupné z: www.dresden-elektronik.de

SEZNAM ZKRATEK

WSN	wireless sensor network (bezdrátová senzorová síť)
IEEE	Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)
WLAN	wireless local area network (bezdrátová lokální síť)
Wi-Fi	wireless fidelity (bezdrátová komunikace)
WiMAX	Worldwide Interoperability for Microwave Access (bezdrátová technologie)
MAC	Linková vrstva
PHY	Fyzická vrstva
FFD	Fully Function Device (plně funkční zařízení)
RFD	Reduced Function Device (zařízení s redukovanými funkcemi)
CSMA-CA	Carrier Sense Multiple Access with Collision Detection (metoda detekce nosné s podporou vyhýbání kolizí)
LQI	Link Quality Indication (kvalita spojení)
NWK	network (síťová)
APS	application (aplikační)
6LoWpan	IPv6 low power wireless personal area network
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
SNMP	Simple Network Management Protocol
PIR	pasivní infračervený detektor
IR	infračervený

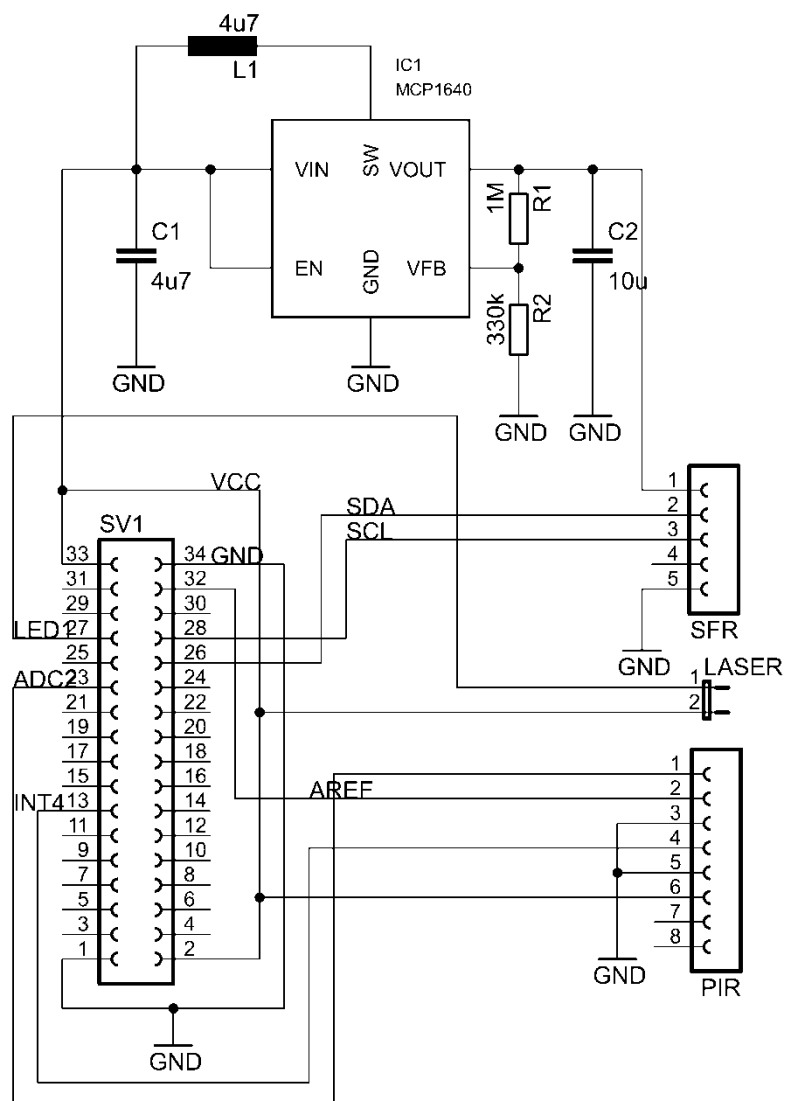
ADC	analogový – digitální převodník
I2C	dvouvodičové datové propojení
PWM	pulzní šířková modulace
JTAG	Joint Test Action Group (rozhraní k testování plošných spojů a k programování)

SEZNAM PŘÍLOH

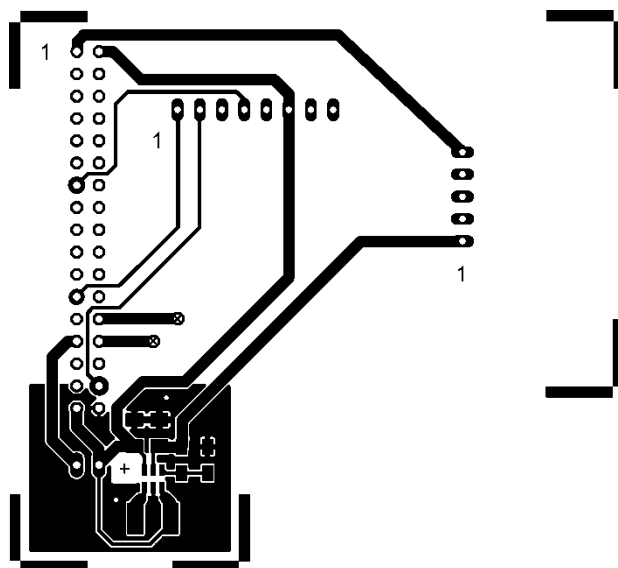
A	NÁVRH ZAŘÍZENÍ	1
A.1	Obvodové zapojení.....	1
A.2	Deska plošného spoje – top	2
A.3	Deska plošného spoje – bottom	2
A.4	Osazovací plán měřiče – top.....	3
A.5	Osazovací plán měřiče – bottom.....	3
B	SEZNAM SOUČÁSTEK	4
C	OBSAH PŘÍLOŽENÉHO CD	5

A NÁVRH ZAŘÍZENÍ

A.1 Obvodové zapojení

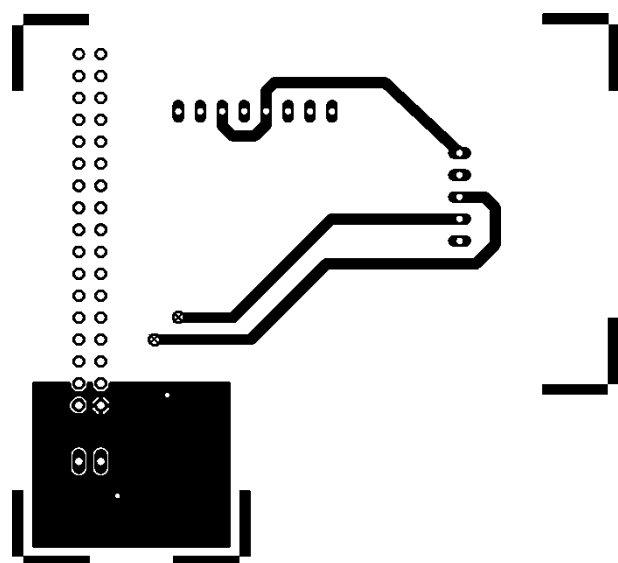


A.2 Deska plošného spoje – top



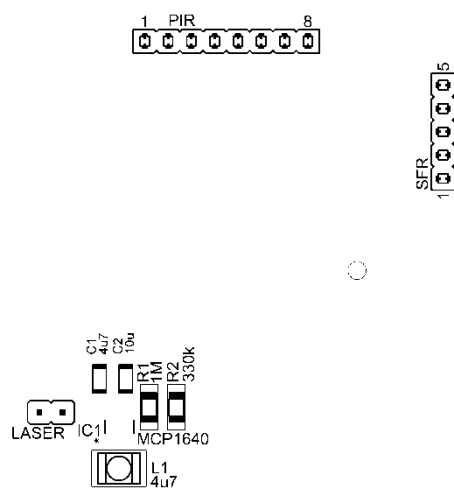
Rozměr desky 68 x 60 [mm]

A.3 Deska plošného spoje – bottom

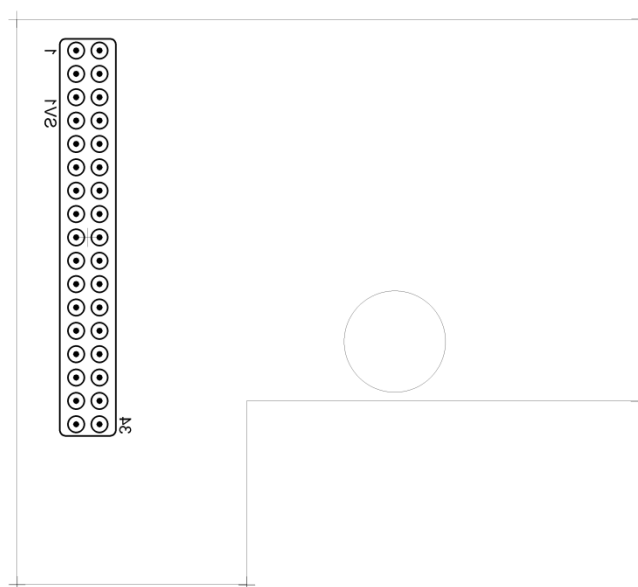


Rozměr desky 68 x 60 [mm]

A.4 Osazovací plán měřiče – top



A.5 Osazovací plán měřiče – bottom



B SEZNAM SOUČÁSTEK

Označení	Hodnota	Pouzdro	Popis
C1	4,7 μ F	1207	Keramický kondenzátor
C2	10 μ F	1207	Keramický kondenzátor
R1	1M Ω	1207	Rezistor
R2	330k Ω	1207	Rezistor
L1	4,7 μ H	1210	Tlumivka
IC1	MCP1640	SOT23-6	DC-DC měnič
SFR		BL805G	Dutinková lišta pro připojení SRF08
LASER		PSH02-02PG	Konektor se zámkem pro připojení Laserového modulu
SV1		BL834GD	Dutinková lišta pro připojení desky k uzlu
PIR		BL808G	Dutinková lišta pro připojení PIR čidla

C OBSAH PŘILOŽENÉHO CD

- Elektronická verze diplomové práce
- Výkresy všech DPS ve formátu pro návrhový program Eagle
- Složka obsahující zdrojové kódy navrženého programu